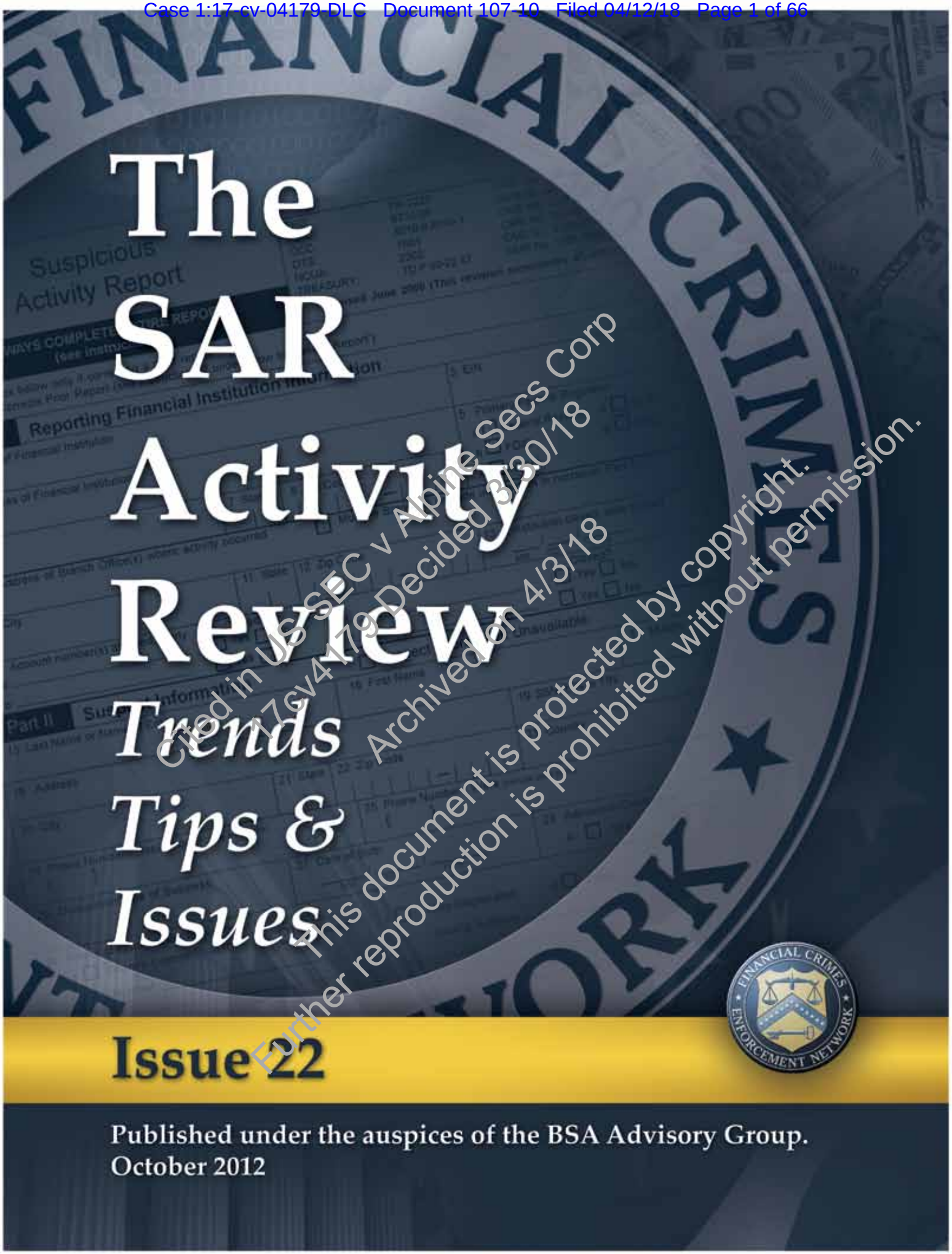


The SAR Activity Review

Trends Tips & Issues

Issue 22

Published under the auspices of the BSA Advisory Group.
October 2012

Financial Crimes Enforcement Network

The SAR Activity Review

Trends Tips & Issues

Issue 22

Published under the auspices of the BSA Advisory Group.
October 2012

Table of Contents

Introduction **1**

Trends & Analysis **3**

SAR Activity Review Customer Satisfaction Survey Results **3**

Foreign-Located Money Services Businesses: An Insight into the foreign-located MSB Population **7**

Law Enforcement Cases **11**

Issues & Guidance **21**

Project STAMP (Smugglers' and Traffickers' Assets, Monies and Proceeds) **21**

Analysis of Suspicious Activity Report (SAR) Inquiries Received by FinCEN's Regulatory Helpline **24**

Suspicious Activity Reports: Back to the Basics **35**

Writing Effective SAR Narratives **38**

Industry Forum **47**

Taking a Second Look at AML Risks from Business Funded Prepaid Cards: It's a Whole New Ball Game **47**

Feedback Form **57**

The SAR Activity Review **Index** is available on the FinCEN website at:
http://www.fincen.gov/news_room/rp/files/reg_sar_index.html
For your convenience, topics are indexed alphabetically by subject matter.

Introduction

The SAR Activity Review – Trends, Tips & Issues is a product of continual dialogue and collaboration among the nation's financial institutions, law enforcement officials and regulatory agencies to provide meaningful information about the preparation, use and value of Suspicious Activity Reports (SARs) and other FinCEN reports filed by financial institutions.

Each year, FinCEN conducts a survey of readers of the *Trends, Tips & Issues* and its companion publication, *By the Numbers*. In the Trends & Analysis section of this issue, we summarize the 2009-2011 ratings and feedback received for the *Trends, Tips & Issues* publication. In this section, we also include an article on foreign-located money services businesses (MSBs) who have registered with FinCEN through August 2012 based on new registration requirements.

In early 2012, FinCEN conducted outreach to all of our state and local law enforcement partners and asked those entities to provide feedback on their use of FinCEN data. The *Law Enforcement Cases* section highlights how access to FinCEN's Gateway system has assisted these agencies in their investigations.

In *Issues & Guidance*, we include an article from U.S. Immigration and Customs Enforcement Homeland Security Investigations' Project Smugglers' and Traffickers' Assets, Monies and Proceeds (Project STAMP). Two articles from FinCEN staff included in this section focus on changes to the new FinCEN SAR and some of its new fields and features. In this section, we also include help for filers in writing more effective SAR narratives, in particular examining SARs involving potentially unregistered MSBs and counterfeit checks.

Finally, in the *Industry Forum*, we get an industry perspective on the AML risks presented by business funded prepaid cards.

As always, we very much appreciate your feedback. Please take a moment to fill in the form at the end of this issue to let us know if the topics we have covered are helpful to you, as well as what you would like to see covered in future editions.

Financial Crimes Enforcement Network

Barbara Bishop
Regulatory Outreach Project Officer
Financial Crimes Enforcement Network

The SAR Activity Review – Trends, Tips & Issues is possible only as a result of the extraordinary work of many FinCEN employees and FinCEN's regulatory, law enforcement and industry partners. FinCEN would also like to acknowledge the members of the Bank Secrecy Act Advisory Group (BSAAG) SAR Activity Review Subcommittee for their contributions to the development of this publication, particularly the Co-chairs noted below.

Helene Schroeder
Special Counsel
Commodity Futures Trading Commission

Michael Cho
Global Head, Anti-Money Laundering Compliance
Northern Trust

Trends & Analysis

This section of *The SAR Activity Review – Trends, Tips & Issues* contains information, such as those identified through analysis of FinCEN reports and calls to FinCEN's Regulatory Helpline.

SAR Activity Review Customer Satisfaction Survey Results

By FinCEN's Office of Outreach Resources

Each year FinCEN conducts a survey[1] of readers of *Trends, Tips & Issues*, along with its companion publication *By the Numbers*. Respondents are asked to answer certain benchmarking questions about the publications and to rate the publications. In rating *Trends, Tips & Issues*, respondents are asked questions about the usefulness of the main sections of the publication, as well as the value of the information in each section based on four criteria: providing guidance on filing requirements; helping improve Bank Secrecy Act (BSA) or anti-money laundering (AML) programs; providing feedback on the use of Suspicious Activity Reports (SARs); and, the opportunity for readers to suggest future topics for the publication.

1. FinCEN uses the services of a federal contractor to conduct the survey and to provide FinCEN a report of the survey findings.
2. Prior to the 2010 survey, FinCEN used contact information provided through regulatory reporting to identify the survey audience. Beginning in 2010, FinCEN developed its list of survey recipients from persons who signed up to receive information on FinCEN publications via FinCEN Updates (available through FinCEN's website), allowing FinCEN to better target readers of the publication for their feedback. This survey covers only the most recent three-year period of surveys.

This article summarizes the ratings received for the *Trends, Tips & Issues* publication for the 2009 through 2011 surveys,[3] and responses to the question: "What would you change to improve *Trends, Tips & Issues*?"

Percentages of respondents who found *Trends, Tips & Issues* useful:			
	2009	**2010**	**2011**
Overall satisfaction	73%	80%	80%
Issues & Guidance	80%	86%	86%
Law Enforcement Cases	74%	83%	82%
Trends & Analysis	70%	78%	78%
Industry Forum	67%	72%	73%

Value of information in *Trends, Tips & Issues*:			
	2009	**2010**	**2011**
Providing guidance on filing requirements	76%	81%	80%
Helping improve BSA or AML program	75%	79%	78%
Providing feedback on the use of SARs	72%	79%	79%
Opportunity to suggest future topics	68%	71%	72%

Key themes from survey responses

In characterizing the written responses to the question of what readers would change to improve *Trends, Tips & Issues*, there were several key themes. Responses were categorized as based either on feedback on each section in the publication or leading trends in the responses, such as length and frequency of each issue, the general style and content of the publication, access to the publication and the focus on a theme for May issues of the publication.

Issues & Guidance

Overall, survey respondents most frequently asked for more tips and guidance, such as how to complete forms, as well as how to avoid common errors and how to write more effective SAR narratives (i.e., narrative examples; key words to use in writing

3. The 2012 customer satisfaction survey was conducted in June, 2012. Results from the 2012 survey are not yet available.

narratives; and, what is beneficial to law enforcement). While some respondents asked for more feedback from regulators as to issues they identify in the field, most wanted to hear from FinCEN in the form of increased regulatory interpretation; information on the status of pending regulations; guidance on strengthening compliance programs (best practices, developing risk assessments); how to apply regulations and guidance; and, clarification of what has changed and what those changes mean for financial institutions.

This issue of *Trends, Tips & Issues* includes an article comparing more effective and less effective SAR narratives reporting potentially unregistered MSBs or the passing of counterfeit checks. In the *Issues & Guidance* section of this issue, we also include information and tips for filers on some of the changes in the new FinCEN SAR form, the use of which will be required early in 2013.

Law Enforcement Cases

The single largest category of responses each year was a request for more (and more detailed) law enforcement cases. Respondents frequently commented on the value of the cases in training employees, and indicated that more detail (i.e., red flags; what led to the institution's identification of the activity and the subsequent SAR filing) would benefit them in identifying suspicious activity being conducted at their institutions. They also indicated they would like to see more variety in the types of institutions and products profiled in the cases. Respondents also frequently requested more feedback on the usefulness of SARs to law enforcement, specifically how they use the reports and statistics on the use of BSA reports in cases.

Unrelated to the survey, in early 2012, FinCEN conducted outreach to all our state and local law enforcement partners and asked those entities to provide feedback on their use of FinCEN data. *The Law Enforcement Cases* section highlights how access to FinCEN's Gateway system has assisted these agencies in their investigations.

Trends & Analysis

Respondents indicated they would like to see less emphasis on statistics and greater emphasis on an analysis of the activity being covered in this section to help in better understanding vulnerabilities and risks. They indicated they would also like to see more information on new typologies, technologies, vulnerabilities and risks – including for products or specific industries – and better information on how to identify, monitor for and investigate these activities, as well as how to report them. They also would like to see more timely information presented in the publication.

Industry Forum

While scoring well for usefulness, readers generally provided very little feedback on this section. Respondents did say they would like to know how other BSA officers use the information contained in the publication (i.e., training), and other such feedback from peers. Several respondents suggested a Q&A forum where readers could submit questions that would be answered in the publication.

General style/content of the publication

Some respondents suggested that the writing could be clearer and more concise, with less technical and legal verbiage. Others commented that they would like to see the formatting changed to an easier to read font and more information on fewer pages (i.e., less white space).

Industry Focus

Many respondents indicated they like the industry focused issues, but don't necessarily want the focus to be on one industry for an entire issue. Instead, they suggested including more industry related topics in each issue – particularly smaller ones (such as community banks and credit unions), and industries that don't receive as much attention (such as precious metals/jewelry and insurance). One respondent suggested doing a feature article on a particular industry (rather than a whole issue), and including articles related to other industries, or content that is then applicable to all industries. Some respondents suggested publishing an issue for each industry. Respondents also expressed an interest in seeing more international focus in the publication's content.

Access to publication/access to previously published information

Several respondents commented on how we notify readers when a new issue is published (via FinCEN Updates), asking if, for example, a PDF of the issue could be sent along with the Update notification. Enhancing the index, which is available online, and improving the ability of readers to find content from past issues were also common requests.

Length & frequency of the publication

Respondents frequently commented that the publication should be shorter, and many suggested including something like an executive summary that would highlight the key points in each section/article – allowing readers to focus on the topics of particular interest to them. Some respondents also thought it should be published more frequently than its current publication schedule of twice yearly (May and October.)

We greatly appreciate the feedback that readers of the publication provide through the annual survey and through the online feedback process. The feedback provided helps FinCEN in identifying enhancements and changes that will increase the value of the publication to its readers, and in identifying future topics for the publication, and we will look for opportunities where we can include these suggestions in future plans for the publication. We encourage readers of the publication to sign up for FinCEN Updates[4] to receive information on when the publication and survey are issued, and to continue to provide feedback.

Foreign-Located Money Services Businesses: An Insight into the foreign-located MSB Population

By FinCEN's Office of Outreach Resources

On July 21, 2011, FinCEN published in the Federal Register a final rule relating to money services businesses (the Final Rule).[5] The Final Rule indicated that an entity may now meet the definition of a money service business (MSB) under the Bank Secrecy Act (BSA) regulations based on its activities within the United States, even if none of its agents, agencies, branches or offices is physically located in the United States. The Final Rule arose in part from the recognition that the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations.[6]

On March 14, 2012, FinCEN made available a new Registration of Money Services Business (RMSB) report. The new RMSB (FinCEN RMSB) allowed for foreign-located entities engaging in MSB activities in the United States to register as an MSB with FinCEN and thus comply with the registration requirement of the Final Rule.

4. Information on subscribing to FinCEN Updates can be found in the "What's New" section of the FinCEN website at www.fincen.gov.
5. Definitions and Other Regulations Relating to Money Services Businesses, 76 FR 43585 (July 21, 2011). http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf.
6. *Id.* at 43588.

FinCEN makes available to the public, through the MSB Registrant Search Web page,[7] the registration information of MSBs submitting an RMSB. FinCEN currently has approximately 37,000 registered MSBs,[8] though this number fluctuates throughout the year as new registrations are processed and businesses that are no longer conducting MSB activities or fail to renew their registration drop off the registration list. In this article, FinCEN examines the characteristics and common trends identified from the registered foreign-located MSB population.

Analysis

The data available in the MSB Registrant Search Web page contains self-reported information from U.S.-based and foreign-located MSBs. As a result, the analysis summarized in this article is based on the information provided, through RMSBs, by foreign-located MSBs. FinCEN staff analyzed the data to identify patterns and trends in the foreign-located MSB population, including geographic location and types of services provided.

Findings

Through August 2012, 80 foreign-located MSBs had registered with FinCEN, and the available data revealed a number of key attributes about the foreign-located MSB population.

Location of the foreign-located MSB Population

A geographic analysis of the foreign-located MSB population showed that the registrants were located only in the Americas or in the United Kingdom, with 72 (90 percent) headquartered in Latin-America. Mexico was home to the highest number of foreign-located MSBs who have registered, followed by Argentina and Uruguay. The majority of registered MSBs from non-U.S. jurisdictions, with the exception of those located in Mexico, were located in their home country's capital city. MSBs from Mexico, notably, originated from 27 states and a federal district.

7. http://fincen.gov/financial_institutions/msb/msbstateselector.html.
8. http://fincen.gov/financial_institutions/msb/msbstateselector.html.

The following map, as well as Table 1, breaks down the number of registered MSBs by country.

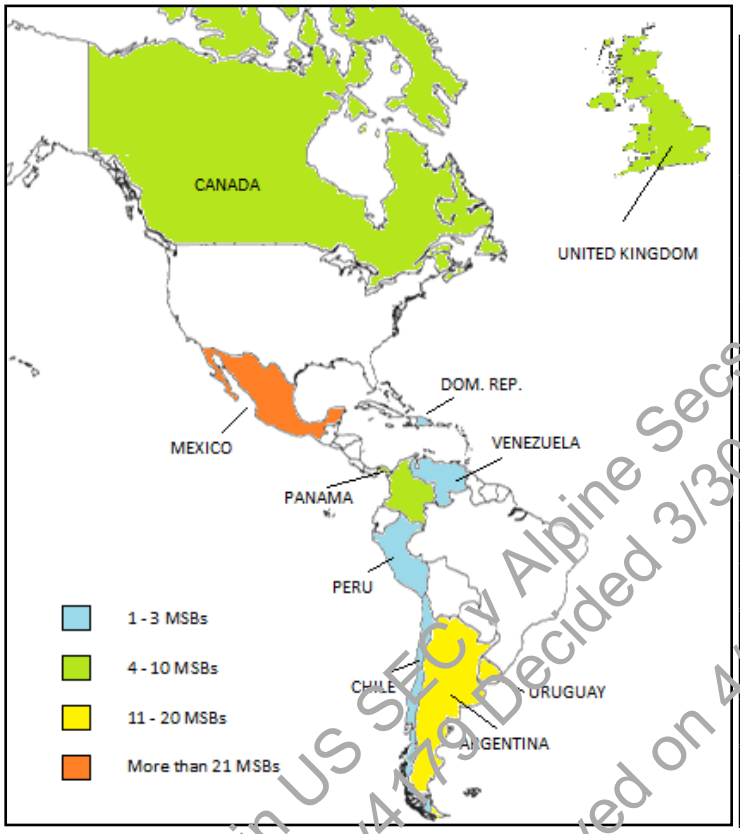


Table 1: Number of MSBs by Country

Country of Locality	*Number of registered MSBs*
Mexico	33
Argentina	12
Uruguay	11
United Kingdom	4
Canada	4
Colombia	4
Panama	4
Venezuela	3
Chile	2
Peru	2
Dominican Republic	1

Services Provided

As part of the registration process, MSBs are asked to indicate the type of MSB activities that they provide or will be providing. Forty five MSBs, or 56 percent of those registered, indicated they offered money transmission services; 41 MSBs, or 51 percent of the population, specified being dealers in foreign exchange; 31 entities, or 39 percent of the registered MSBs, said they provided check cashing services. The registration information also revealed that 37 foreign-located MSBs, 46 percent of the population, engaged in more than one type of MSB activity. Most notably, 31 MSBs indicated that they offered both check cashing and foreign exchange services.

Table 2 shows the totals reported for each category of MSB activity listed.

Table 2: Number of MSBs by Activity

Category of MSB Activity Reported	*Number of registered MSBs*
Check Cashier	31
Money Transmitter	45
Seller of Prepaid Access	1
Provider of Prepaid Access	1
Dealer in Foreign Exchange	41
Other	5

Geographic Location and the type of Services Provided

The available data contained a large number of foreign-located MSBs that engage in more than one type of MSB activity; however, certain patterns of behavior emerged based on the MSB's geographic location.

Contrasting patterns were observed when comparing MSB activities offered by those located in Mexico to those offered in almost any other country. Nearly all of the MSBs located in Mexico offered both check cashing and foreign exchange services. MSBs in Argentina, Uruguay, Panama, United Kingdom, Colombia, Venezuela, Peru, Chile, and the Dominican Republic tended to provide money transmitting services. Moreover, the only registered provider and seller of prepaid access was located in the United Kingdom. The activities in which certain MSBs engage may be representative of local population trends as these entities strive to meet the demand of their customer base.

Conclusion

FinCEN will continue its outreach efforts in order to help entities engaging in MSB activities to understand their BSA/AML obligations. FinCEN expects the number of registered foreign-located MSBs to increase as the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations.[9] As additional foreign-located MSBs register with FinCEN, the registration information that will be provided will contribute significantly to a better understanding of the foreign-located MSB population and the services they provide.

9. Definitions and Other Regulations Relating to Money Services Businesses, 76 FR 43588 (July 21, 2011). http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf.

Law Enforcement Cases

In this section of *The SAR Activity Review* we summarize cases where FinCEN information played an important role in the successful investigation and prosecution of criminal activity. Law enforcement case examples can be found on the FinCEN website under the link to Law Enforcement. This site is updated periodically with new cases of interest. The index of cases are listed by the type of form used in the investigation, type of financial institution involved, and type of violation committed.

Contributing editors: Shawn Braszo, Don Battle, Sean Donnelly, Jim Emery, and Jack Cunniff.

Since its creation in 1993, FinCEN's Gateway program has served as the primary vehicle for state and local law enforcement to access FinCEN records. Originally, FinCEN established coordinators in each state to access records on behalf of law enforcement in their jurisdiction. As recognition of the value of FinCEN data grew, some major metropolitan police departments, as well as some statewide agencies, requested their own access to the data. Today, querying FinCEN records in state and local investigations is a common occurrence.

In early 2012, FinCEN conducted outreach to all of our state and local law enforcement partners and asked for cases where FinCEN data played a useful role in their law enforcement investigations. We received many case examples from our state coordinators, state agencies and local departments in response to our outreach.

Below, *in their own words*, are just some examples of how our stakeholders use FinCEN data. These examples have been edited only for confidentiality and privacy concerns.

State Coordinator Cases

State Coordinators are the primary contact points for local and state law enforcement agencies to obtain FinCEN records. Depending on the state, the coordinator could be the attorney general, state police, or the department of public safety. Frequently, the state coordinators are the primary contact point for a variety of resources that can benefit law enforcement agencies.

Identity Theft

"A local credit union began receiving online applications in January of 2010 for new accounts allegedly from females residing in a major metropolitan area. Similarities in the online account applications started becoming apparent after fictitious checks were deposited via ATMs shortly after the accounts were opened. It was discovered that each account was opened with a fictitious driver's license (the names and personal identifying information were real), included previous addresses in another state, and came from IP addresses that were from the same location and provider. One last application was received for a business account with a local address, but the business owner resided out of state. The application came from an IP address in the same location as the previous applications. Surveillance video from the ATM deposits into the accounts appeared to be the same person, sometimes carrying a small dog with a white car in the background which matched the business owner's Facebook photos of herself, her dog, and her new car. The females, whose names appeared on the previous online accounts, were contacted and it was verified that they were identity theft victims. One of the victims had previously worked for the suspect.

The credit union investigator requested the assistance of a state law enforcement unit and a federal agency. Numerous SARs were found and helped to identify other financial institutions having similar activity with the same suspect, identified more identity theft victims, and pointed to other ongoing criminal investigations throughout the metro area. Further investigation identified associated persons and the identity theft ring was tied to several other criminal investigations involving the use of stolen personal and financial information to open credit accounts in several local jewelry stores where the members of the organization purchased several high-end pieces on credit which were later pawned for cash.

A grand jury indicted the group consisting of the ring leader and four others. The ring leader was sentenced to 20 years in prison."

Welfare Fraud

"A request for a FinCEN commercial database, CTR, and SAR request was received from a county prosecuting attorney's office regarding foreign nationals suspected of committing welfare fraud. Information gathered indicated that the foreign nationals had set up a cleaning business on Craigslist that involved wire transfers made through Western Union. It was reported that one of the suspects involved may have been in the United States illegally. The suspects were purported to have also engaged in welfare fraud in another state.

The information obtained from FinCEN was instrumental in the on-going investigation of the welfare fraud case and also resulted in the deportation of the illegal persons."

Embezzlement

"A plastic surgeon discovered an embezzlement scheme by his bookkeeper when, during the bookkeeper's vacation, he learned of his overdrawn account. The bookkeeper had attempted to evade detection of the embezzlement by destroying, inter alia, bank records and tax deficiency notices. FinCEN records led us to request all records for the subject's gaming activity from local casinos and we established that the subject had been embezzling for over 5 years to support her gambling habit. Upon our establishing an embezzlement of over $300,000 the subject took a nolo contendre plea and received a sentence of 20 years suspended after 78 months."

Fraud

"A local police department received a complaint from a woman who had fallen victim to an advance-fee lottery scheme perpetrated by an individual from another state. FinCEN matched the local investigator to that state's law enforcement community and we discovered that the out-of-state perpetrator had in fact been victimized by others who had pressed him to send money overseas. FinCEN records were critical in helping local police coordinate their efforts with the other state's law enforcement agency, helping to save valuable man-hours at the local level."

Elder Abuse (Financial)

"FinCEN data was critical in identifying the disposition of a $20,000 withdrawal from a bank account of elderly persons. Investigators had earlier executed a search warrant for the records of the victims at the bank that had filed the CTR but the bank had inadvertently missed the transaction in question. The discovery of the CTR resulted in us urging the bank to complete its compliance with the initial search warrant. Records pertaining to the cash withdrawal helped arrest the subject on charges of larceny totaling $218,000."

Cases from an Attorney General's Office

Case A

"The defendant owned gas stations, and following an investigation by the department of revenue the defendant was indicted on multiple counts of fraud related to sales and tax records.

A FinCEN search was conducted on the defendant and the defendant's businesses. Information obtained through FinCEN established that the defendant had made numerous large cash deposits during the period of time covered by the indictment. The defendant was confronted with this information. Shortly thereafter, the defendant pled guilty to all charges.

In addition, the defendant claimed he had no assets. The FinCEN searches identified financial accounts controlled by the defendant. This information was vital at sentencing. The defendant was sentenced to a period of probation and ordered to pay almost $1 million in restitution."

Case B

"The defendant was the former president of a technology firm. The defendant executed a false billing scheme involving multi-million dollar contracts with the state for drug testing. During negotiations with the defendant to settle a false claim suit, the defendant asserted that her assets had dissipated. FinCEN searches provided account and deposit information of accounts controlled by the defendant. This information was important in obtaining a settlement of almost $400,000 in restitution to the state."

Case C

"A FinCEN search of the defendant company identified a Suspicious Activity Report. The information contained in the SAR was used to track down additional loan transactions. Interviews of newly identified victims led to the filing of an Amended Complaint naming the owner of the mortgage company as a defendant and individually liable. Shortly thereafter, the case settled with $7,500 in restitution and a $10,000 civil penalty."

State Agency Cases

FinCEN maintains Memoranda of Understanding with some state agencies that have criminal investigative authority in matters such as taxes, revenues, and gambling. Typically, these agencies requested FinCEN data so frequently that they tended to overburden the state coordinators. Based on the agencies' mission and use of the data, FinCEN provides access to ensure that BSA material is used to its fullest extent.

Insurance Fraud

"I am a crime intelligence analyst in the fraud division currently assisting my detective on a worker's compensation case that involves a check cashing company. We decided to look at the companies that have cashed the largest number of checks at this particular check cashing establishment. We wanted to see if in fact the amount of payroll cashed was equivalent to what was reported to the worker's compensation insurance carrier. After getting the worker's compensation coverage information, I realized that the company did not have any coverage in over 3 years. I was a bit disappointed because I was hoping the company was still in business and active in cashing checks, otherwise the case would not pan out to be much of anything.

The decision to run a FinCEN report on the company was made, and lo and behold, CTRs for this particular company have been nonstop through and including those years they were not covered by worker's compensation insurance, including a recent transaction. Our investigation received a boost thanks to FinCEN."

Money Services

"Our money service business squad considers the FinCEN intelligence as invaluable to their work. Without it, there would be no MSB investigations. The vital reason for using the FinCEN intelligence is that it identifies some of the filers as known criminals, which in turn incriminates the money service businesses that they are utilizing. The financial analysis on FinCEN also corroborated the days of the week when the criminal activity occurs most frequently."

Taxes

"This case involved a doctor who had not accurately reported his true income filed on state and city business and personal income tax returns for several years. As a result of "mining" FinCEN data, we discovered this doctor had moved over $3 million to accounts in offshore locations. The source of this money was diverted insurance payment checks that were initially deposited into personal accounts and then forwarded offshore. Further investigation determined this money had not been reported on the business or personal income tax returns. It was also discovered that he distributed money into domestic accounts held in his children's names and into other investment accounts.

After reviewing subpoenaed bank account information and 1099 statements from insurance companies, we determined the doctor had underreported his income by more than $6 million for tax years 2005 through 2009. The doctor learned of the investigation through one of the subpoenaed financial institutions. His counsel contacted the prosecutor's office and indicated his client wanted to pay his full tax liability and take responsibility for what he had done wrong."

Local Municipality Cases

Local police and sheriff agencies increasingly use FinCEN records in their investigations. Many local agencies have representatives on SAR review teams and task forces that share FinCEN data. In addition, FinCEN has given direct access to some local agencies with a robust financial crime focus that have a history of using the data.

Illegal Exports

"While investigating subjects of interest because of previous criminal activity, local detectives and federal agents found multiple SARs indicating (cash-in) illicit structured transactions designed to avoid reporting requirements. Investigators found SARs filed in a 2-year period on a pilot and operator of a passenger jet charter service operating from a townhouse residence in the local area, detailing a pattern of structuring.

After reviewing numerous SARs, detectives noted that from in a 14-month period, there were two hundred and fifty three (cash-in) structured deposits totaling approximately $1.7 million.

In addition, other SARs noted that the main subject used approximately 16 bank accounts titled in his name, the names of his family members, friends or business associates, or names of companies owned by him, family members or business associates to make the placement of the structured cash deposits.

After the initial structured cash deposits, the SARs noted that the funds were combined and moved from the initial account to or through one or more of the associated accounts to layer prior to being transferred to destination accounts. Subsequently, the pooled funds were transferred from the destination accounts to the escrow account of the respective aircraft title companies to purchase aircraft as the final step in the integration process.

Based on SARs, detectives subpoenaed and reviewed video bank surveillance tapes. The video bank surveillance clearly noted that two bank employees assisted in the structured cash deposits to include knowingly and willfully failing to file a Currency Transaction Report, as required by law.

A bank legal internal investigation was initiated and upon completion, a total of 11 bank employees were terminated. The main bank official (a subject associate) was later indicted for conspiracy to commit money laundering.

Following one of the money trail in this investigation, also led to a personal check that was traced to a freight forwarding company. Further investigation revealed that the check was payment for shipment of an exported container. A subpoena was served upon the freight forwarding company for any and all documents related to the subjects. Review of those documents uncovered that the subjects exported 11 stolen boats. This information was forwarded to federal agencies which assisted in the indictment of four additional targets in another criminal investigation.

As a result of this SAR investigation, detectives seized 32 bank accounts, two Lear jets, three high-end vehicles and obtained probable cause for a search warrant for the subject's residence which resulted in the seizure of additional bulk cash discovered hidden in the attic. The case further resulted in seven state arrest warrants being issued. All but one arrest warrant were served, the seventh subject escaped prosecution by fleeing out of the country."

Failure to Follow Reporting Requirements

"An investigation was initiated on a jewelry and pawn store and its owner due to information obtained by a confidential source (CS). According to the CS, the store was a money service business that was assisting in the laundering of illegal gambling proceeds by cashing checks over $10,000 without complying with the reporting requirement as mandated by the U.S. Department of Treasury. Either the Currency Transaction Report (CTR) was never filed or, the information listed on the CTR was intentionally incorrect and misleading. The owner also provided the CS with a list of nominee names that should be used as payees on the checks in order to conceal the identity of the persons cashing the checks. The owner was aware that the checks being cashed by these individuals were from illicit gambling proceeds and would charge 4 to 6% of the checks in order to cash them and violate the reporting requirement for these individuals, instead of her normal fee of 2 to 3% for legitimate customers.

In order to verify the validity of the information, an undercover operation was initiated which targeted the store and its owner. The undercover officer (UO) was introduced to the owner by the CS as an individual needing checks cashed without the filing of a CTR. The UO then cashed numerous checks at the business with the owner that were each over $10,000. The checks were intentionally made payable to a false nominee name, which was on a list of names provided by the owner. When the checks were cashed by the UO, the owner failed to obtain his identification for the CTR and cashed the checks anyway. The owner charged the UC 4% for each check cashed. Three checks were cashed by the UO in this manor totaling $33,000. Using the FinCEN data base, it was confirmed that the owner failed to file the CTRs for the three checks cashed by the UC at her business.

In addition to the undercover operation, a financial analysis of the business bank accounts for the years 2008-2009 revealed 105 checks cashed at the business that were all over $10,000. A FinCEN data base check revealed that these transactions either did not have a corresponding CTR or the CTR that was filed had inaccurate information concealing the identity of the person receiving the cash. The total dollar amount of checks cashed by the owner that violated the reporting requirement was $3.2 million dollars for the years 2008-2009.

As a result of using the FinCEN database, this case resulted in the state prosecution and the seizure of almost $150,000."

Narcotics Trafficking, Money Laundering, and Mortgage Fraud

"Beginning in 2009, a major drug investigation was established on targets who were a group of narcotics traffickers in the local area.

While conducting FinCEN checks, a number of CTRs and 8300s were observed on the main targets. The CTRs led this detective to the targets' main bank accounts, and through subpoenas, we were able to identify assets that had been purchased with laundered funds from narcotic sales. The 8300s also identified assets that were later seized reference to being purchased with laundered funds from narcotic sales.

Four subjects were arrested and charged with Title 21 U.S.C 963 Conspiracy to Import at least 5 Kilograms of Cocaine, and Title 18 U.S.C 1956 Money Laundering. One subject was charged with bank fraud. Approximately $1.4 million in property and assets were seized and all subjects have pleaded guilty and are serving their sentences in federal prison."

Stolen Cars

"Members of the county police department has been conducting a joint investigation targeting a multi-spectrum stolen/carjacked vehicle exportation organization.

During the months of March and April, 2011, the police department conducted an investigation into the purchasing of stolen and carjacked vehicles from within the county that were being exported to Africa. During the investigation, several suspects were identified as key members of the operation. FinCEN queries were conducted, and this information was used to confirm and identify additional locations for the suspects operation. Due to this information, numerous search and seizure warrants were executed and stolen property was recovered, along with the arrests of three suspects.

The three suspects in this case were subsequently charged in U.S. district court where they have pleaded guilty and have received federal prison sentences."

SARs/CTRs Lead to Asset Forfeiture

"While investigating an alleged robbery at an upscale hotel, local law enforcement officials identified the complainant of the alleged robbery as a suspected drug trafficker. The initial investigation also resulted in the on scene-seizure of currency in excess of $131,000. Asset forfeiture investigators found SARs filed in 2010 and 2012, as well as CTR information filed during 2011, directly associated to the defendant.

This SAR and CTR information assisted investigators with the identification of bank accounts and detailed the structuring of funds. Specifically, within a 2-year period, the

defendant structured more than $246,000 by means of cash deposits and cash withdrawals. The defendant had no record of legitimate employment and provided investigators with conflicting information as to the origin of the $131,000.

As the investigation progressed, the defendant attempted to bribe several law enforcement officials in an attempt to avoid criminal charges. Preliminary investigation did not identify any accounts subject to seizure and/or forfeiture, at present. The defendant's criminal history for trafficking controlled dangerous substances, combined with current evidence of marijuana possession, drug ledgers for bulk sales of marijuana distribution, and evidence refuting the alleged robbery resulted in the forfeiture of the aforementioned seized currency."

Drugs and Money Laundering

"In October of 2010, while observing a vehicle with an out of state registration and heavily tinted windows traveling in the Northwest quadrant of the city, officers conducted a traffic stop on the vehicle. A registration check on the tags revealed that the tags had been suspended. After observing what appeared to be marijuana on the floor of the vehicle in front of the front seat passenger, the officers asked the owner for consent to search the vehicle. The vehicle was occupied by three men.

A search of the vehicle uncovered over $16,000 in U.S. currency and $53,000 in money orders from various locations within the city. The money orders were in various denominations and had all been purchased within a 2 to 3-day time frame. The vehicle's owner was arrested for having an unregistered vehicle. Seized from the driver was an additional $150 in U.S. currency. All the currency and money orders were seized for civil forfeiture processing. Additionally, further investigation into the matter led to the issuance of a search warrant for the driver's local address. Seized as a result of the warrant was an additional $5,953 in U.S. currency, fifty-four and three-tenths (54.3) grams of marijuana, and thirty Oxycodone pills.

As a result of the financial investigation, a FinCEN Gateway query revealed possible "smurfing" activities by the vehicle's owner. This information assisted in the administrative forfeiture of both the currency and money orders."

Issues & Guidance

This section of *The SAR Activity Review* discusses current issues, including those raised with regard to the preparation and filing of SARs, and provides guidance to filers.

Project STAMP (Smugglers' and Traffickers' Assets, Monies and Proceeds)

By United States Immigration and Customs Enforcement Homeland Security Investigations

Project Smugglers' and Traffickers' Assets, Monies and Proceeds (Project STAMP) is a U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations' (HSI) enforcement initiative aimed at targeting the illicit proceeds earned by human smuggling and human trafficking (HS/HT) organizations. These criminal networks create substantial risks to the security of the United States.

In an effort to make sure that HSI utilizes the full thrust of the authorities granted to them as a result of the creation of the Department of Homeland Security (DHS), HSI launched Project STAMP to:

(1) Attack organizations involved in HS/HT from an aggressive anti-money laundering stance. Following the money trail will assist HSI in the identification of key members of criminal organizations involved in HS/HT activity, as well as the identification of assets, monies and proceeds derived from or used in support of their criminal activity; and,

(2) Ensure the seizure of these assets, which is crucial to shutting down entrenched criminal activity.

HSI has already identified a multitude of methods to hide, move and store illicit proceeds associated with illegal activity, including financial institutions, money services businesses, bulk cash smuggling organizations, etc. Seizing the funds that motivate and amplify the problems associated with these organizations is a high priority for HSI and DHS.

HSI continues to explore ways in which the government and the private sector can productively partner together to better identify and report on the suspicious transaction activity related to HS/HT organizations. HSI's efforts related to Project STAMP are in accordance with the guiding principle within DHS's Strategic Plan of building trust through collaboration and partnerships.

As part of Project STAMP, HSI aims to continuously identify and disseminate typologies/red flag indicators related to money laundering by HS/HT organizations. The goal is to map out how these organizations use the financial sector, both domestically and abroad, to collect payment for illegal services rendered and to share these methods with the financial community, ultimately resulting in the shutting down of identified vulnerabilities. A preliminary review of both active and closed HS/HT investigations has identified the following red flag indicators of suspicious financial transactions associated with HS/HT organizations:

- Structuring both deposits and international wires to avoid currency transaction reports;
- Bank accounts being opened for businesses where the customer does not appear to have any involvement in activities related to the business;
- Bank accounts opened in the name of companies that do not have any genuine business activities that are consistent with the type of company they claim to be;
- Wire transfers from one business account to another that have no apparent ties;
- Multiple ATM withdrawals at the daily maximum amount (in this case, $1,000 per day);
- The use of credit card processing accounts with corresponding business fronts with even number charges credited to the account ranging from $300 to $5,000 dollars;
    - Credit card payments to online escort services for advertising. These include small posting fees to companies such as Craigslist as well as more expensive, higher-end advertising and website hosting companies.
- Numerous BSA filings by multiple financial institutions;
- Large cash deposits inconsistent with business type;
- Large payments to foreign companies that are inconsistent with the amount of

product received from these companies;

- Unusual withdrawal, deposit or wire activity inconsistent with normal business practices, or dramatic and unexplained change in account activity;
- Sudden change in customer's normal business practices, i.e., dramatic increase in deposits, withdrawals or wealth;
- Structuring financial transactions at money service businesses (MSBs) (multiple financial transactions structured under the $3,000 MSB's reporting limit on the same day); and
- Numerous incoming wire transfers or personal checks deposited into business accounts with no apparent legitimate purpose.

The success of Project STAMP is integral to our mission of protecting the homeland by shutting down criminal organizations that seek to exploit individuals through smuggling or trafficking schemes. This enforcement initiative is impacting criminal organizations as a whole, by targeting the methods by which these organizations move and launder money to support their illegal activity.

Protecting the United States is more than just a responsibility for government agencies; it's a shared mission for all Americans. The importance of private sector partnership in this shared mission cannot be overstated. There are several ways individuals and businesses can help:

- **Partner** – Become a private sector partner with HSI by contacting your local HSI Special Agent in Charge office and arranging a Cornerstone presentation for your business or organization;
- **Report** – Report suspicious financial, commercial or trade activity by contacting your local HSI Special Agent in Charge office, or by calling 1-866-DHS-2-*ICE*; and,
- **Subscribe** – Sign up for HSI's quarterly newsletter, *The Cornerstone Report*, for new developments in financial and trade fraud crimes.

HSI is the largest investigative agency in the Department of Homeland Security. HSI's mission is to conduct criminal investigations by utilizing our investigative authority to protect the United States against terrorist and other criminal organizations who threaten our safety and national security; to combat transnational criminal enterprises who seek to exploit America's legitimate trade, travel, and financial systems; and

to uphold and enforce America's customs and immigration laws at and beyond our nation's borders. To learn more about Project STAMP and how you can contribute to the shared mission of Homeland Security, visit www.ice.gov/cornerstone.

Analysis of Suspicious Activity Report (SAR) Inquiries Received by FinCEN's Regulatory Helpline

By FinCEN's Office of Outreach Resources

FinCEN operates a Regulatory Helpline that provides assistance for financial institutions seeking clarification of their obligations under FinCEN's regulations implementing the Bank Secrecy Act (BSA) and certain requirements of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act and other statutory authorities.[10] This article provides financial institutions with guidance and instruction regarding the proper completion of the new FinCEN Suspicious Activity Report (FinCEN SAR). The article specifically addresses common inquiries that the Regulatory Helpline received regarding completion of the FinCEN SAR and provides a compilation of additional helpful guidance and instruction.

FinCEN SAR Filing Guidance and Instructions

Between July 1, 2011 and June 30, 2012, the Regulatory Helpline received 1,690 inquiries associated with FinCEN's SAR regulations or requesting assistance in filing a SAR. Since March 29, 2012, when financial institutions began submitting the FinCEN SAR using FinCEN's BSA E-Filing System, approximately one in four of all SAR inquiries have been directly associated with completion of the FinCEN SAR.

Effect of FinCEN SAR on existing regulatory obligations

A common theme among these FinCEN SAR inquiries was uncertainty regarding the status of FinCEN's SAR regulations and compliance requirements. Financial institutions repeatedly sought reassurance that the underlying reporting obligations had not changed with the issuance of the new, electronic-only FinCEN SAR. FinCEN publicly clarified this fact by issuing guidance on the use of new FinCEN

10. Financial institutions can contact FinCEN's Regulatory Helpline at 800-949-2732 or by e-mailing BSA_Resource_Center@fincen.gov.

SAR (and FinCEN Currency Transaction Report or CTR) when the new reports began to be accepted. Specifically, the guidance noted that the FinCEN SAR (and FinCEN CTR) "does not create new obligations or otherwise change existing statutory and regulatory expectations of financial institutions."

Deadlines for adopting the FinCEN SAR and mandatory e-filing

Following the initial release of the technical specifications for the new FinCEN SAR on September 29, 2011, and the proposal mandating the electronic filing of reports submitted to FinCEN, industry raised concerns in its comments to the mandatory e-filing proposal regarding the potential challenge on meeting both requirements simultaneously no later than June 30, 2012. FinCEN provided substantial clarification on the interplay of these two separate, but related requirements in a notice that established the deadline by which financial institutions must adopt the electronic-only FinCEN SAR to be March 31, 2013, while restating the expectation that mandatory e-filing would be required as of July 1, 2012. That notice also made clear that until March 31, 2013, financial institutions could continue to file the older or "legacy" versions of the industry-specific SARs. However, institutions may begin filing on the FinCEN SAR prior to March 31, 2013. The final notice establishing the requirement of mandatory electronic filing for all reports submitted to FinCEN, with certain limited exemptions, cemented that deadline as July 1, 2012.

As of July 1, 2012, therefore, all financial institutions, unless granted a specific limited-time exemption from FinCEN, must file all SARs electronically. Institutions filing paper SARs will be informed of their error and may be subject to civil money penalties for continued reporting requirement violations. Starting April 1, 2013, all financial institutions must file the FinCEN SAR. At that point, no electronically filed legacy SARs will be accepted.

Common filing assistance inquiries

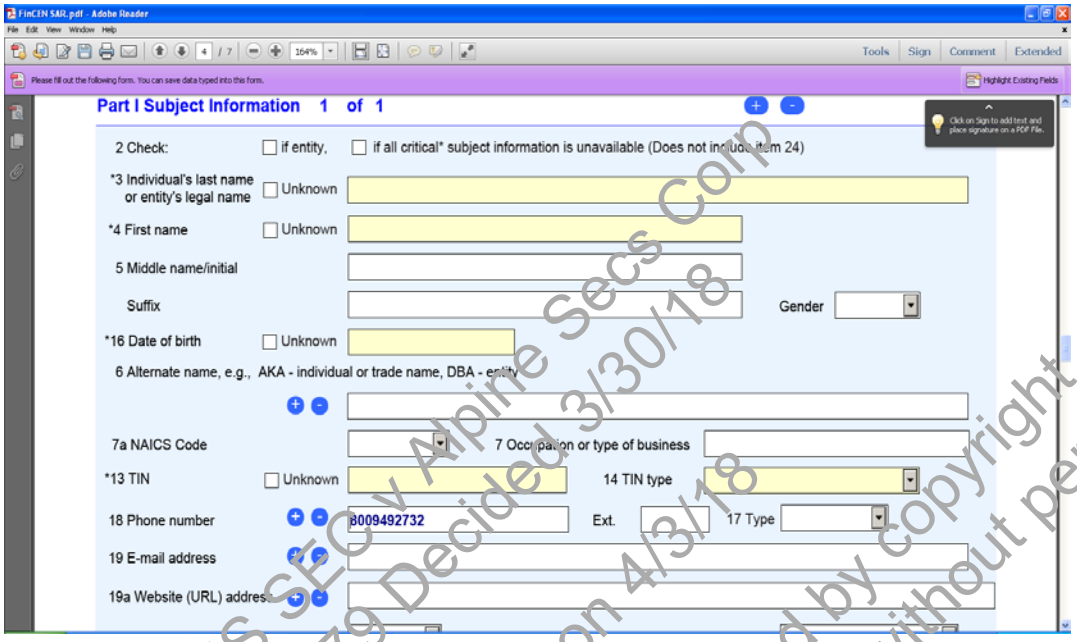
To assist financial institutions in their adoption of the new FinCEN SAR, FinCEN's Regulatory Helpline and E-Filing Help Desk have been responding to a variety of technical and regulatory-related inquiries regarding the new report. The remainder of this article provides helpful guidance, instructions, and other information for financial institutions regarding the appropriate way to complete a FinCEN SAR. In particular, we focus on how to complete a specific "Step" or "Item" with the new FinCEN SAR, much of which can be found in the guidance documents and notices highlighted earlier in this article or within Appendix C of the FinCEN SAR

technical specifications that are located at http://bsaefiling.fincen.treas.gov/news/FinCENSARElectronicFilingRequirements.pdf. Financial institutions are also able to review and download the test copy of the FinCEN SAR to assist in their efforts to adopt the new standard format by accessing FinCEN's BSA E-Filing System user test site at http://sdtmut.fincen.treas.gov/news/SuspiciousActivityReport.pdf. Additionally, this publication includes another helpful article providing general guidance on compliance with FinCEN's requirements when using a FinCEN SAR and a further article explaining how to complete a well-written FinCEN SAR narrative. Finally, FinCEN has made available a recorded webinar addressing most of the same questions and areas of guidance for completing the FinCEN SAR included in this article http://www.fincen.gov/whatsnew/html/20120928.html.

Miscellaneous inquiries related to all Steps and/or Items

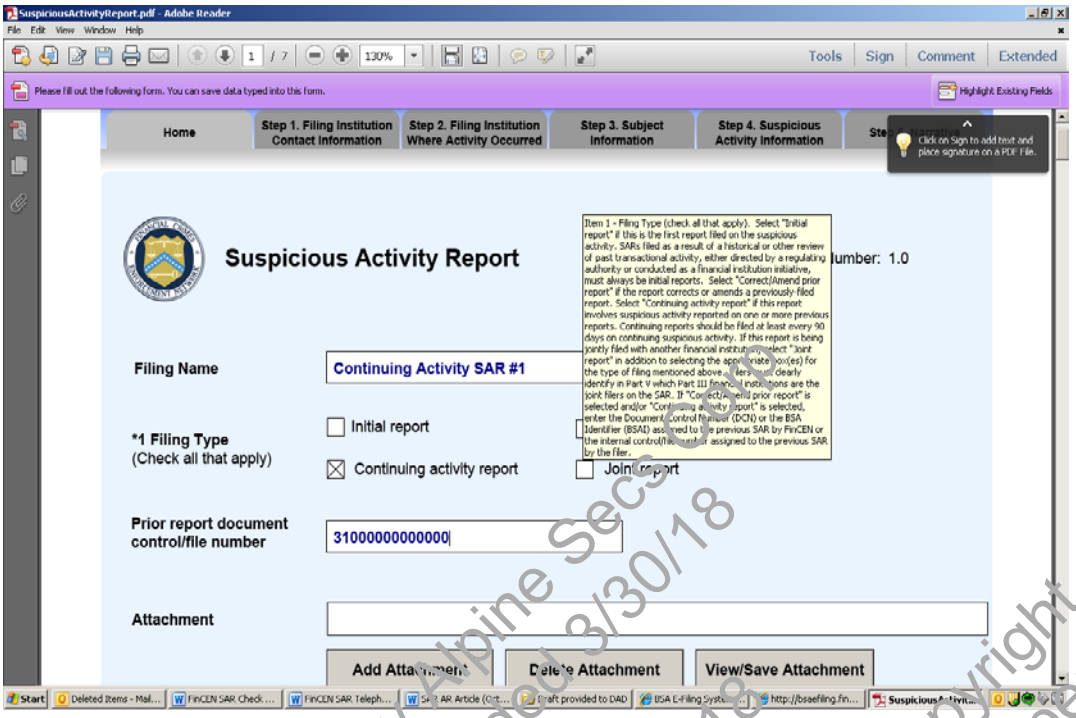
- **When do you check the "Unknown" box?** Financial institutions should file all FinCEN Reports with complete and correct information. However, if an Item is unknown, leave that Item blank and check the "Unknown" box.
- **Are Items without an asterisk required to be completed?** Items with an asterisk ("*" or Items displaying a "yellow" field) are critical fields that the filer is required to complete before the FinCEN Report can be submitted electronically. If an Item does not have an asterisk, it is not a critical field. However, financial institutions should file all FinCEN Reports with complete and correct information. As noted above, if an Item is unknown for a critical field, the institution must check the associated "Unknown" box or the electronic filing cannot be submitted.
- **What if the report requires multiple Steps or Items of the same section, such as branch information, subject information, and financial institution information?** If a particular FinCEN SAR requires multiple Steps and/or Items of the same section, the filer would click the "+" button to create additional Steps and/or Items. Batch filers would add additional records of the same type. For example, there would be multiple 2C records for activity occurring at multiple branch locations, multiple 4A records to accommodate more than one suspect, and multiple 2B records if more than one financial institution was involved.

- **How do you enter data that is formatted, such as phone numbers and identifying numbers?** Enter all identifying numbers as a single text string without formatting or special characters such as hyphens or periods. The below example demonstrates how a phone number would appear.

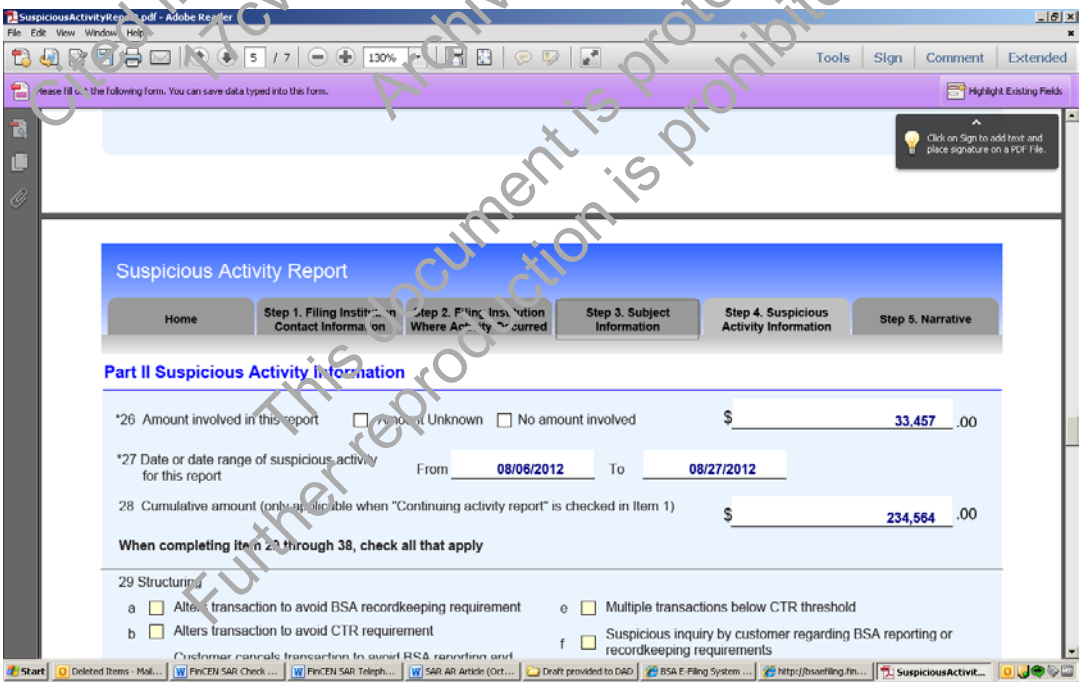


- **When/How do you file a report for continuing activity?** In the May 2012 SAR Activity Review (Issue 21), FinCEN provided guidance on regulatory obligations regarding filing a SAR on continuing activity which explain the timing of when the activity should be reported and the deadlines for the SARs. http://www.fincen.gov/news_room/rp/files/sar_tti_21.pdf.

  The FinCEN SAR has made the reporting of continuing activity easier for filers. In Item 1 (Filing Type), filers must check the "Continuing activity report" box to denote that the report is on continuing activity. The filer should include the prior report Document Control Number or File Number to associate the current filing with the past report.



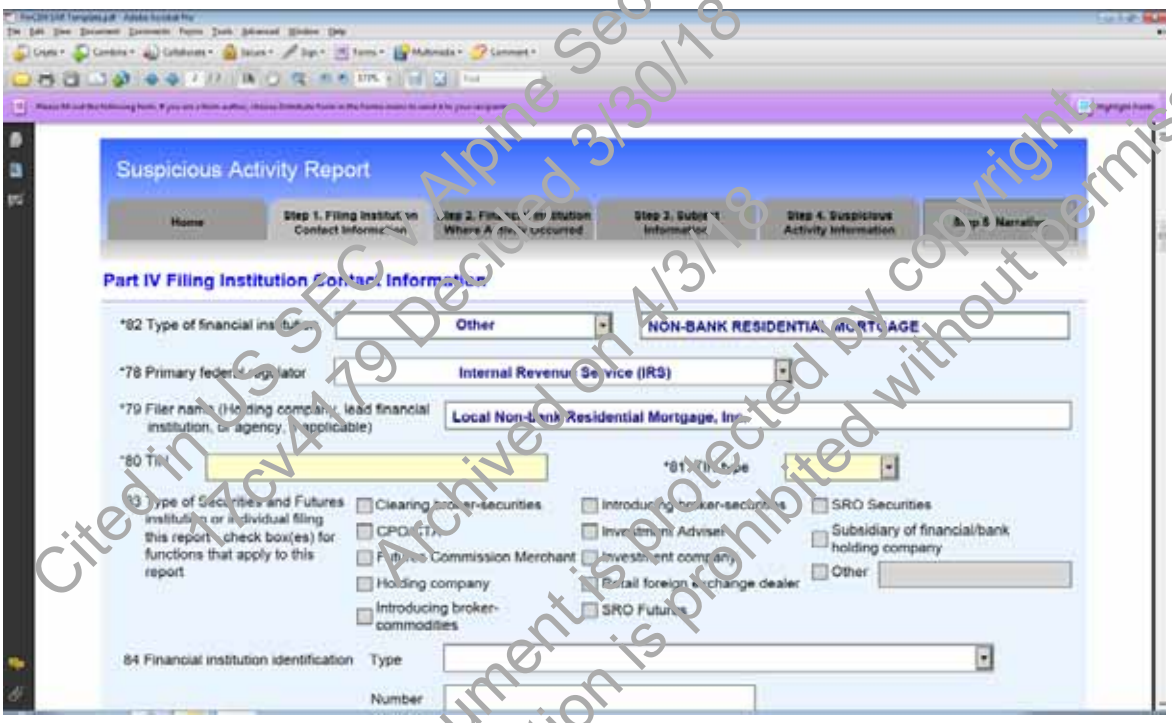
Then, in Item 28 (Cumulative amount), filers can enter both the amount associated with the suspicious activity being reported within the filing but also separately enter the cumulative amount for all the continuing activity (note, this Item is only applicable when the "Continuing activity report" box is checked in Item 1).



Inquiries related to Items in Step 1 (Filing Institution Contact Information)

- **"Type of financial institution" (Item 82)** – Select the option that identifies the type of financial institution entered in Item 79 (Filer name). If none of the options apply, select "Other" and enter a brief description in the associated text field.

  If the financial institution is a non-bank residential mortgage lender or originator, select "Other" and enter "NON-BANK RESIDENTIAL MORTGAGE" in the associated text field. If the financial institution is a dealer in precious metals, stones, or jewels, select option "Other" and enter "DEALER IN PRECIOUS METALS STONES JEWELS" in the associated text field.



- **"Primary federal regulator" (Item 78)** – Select the appropriate option from the drop-down list to identify the Primary Federal Regulator or BSA Examiner of the filing institution. If more than one regulator option could apply, select the regulator that has primary responsibility for enforcing compliance with the BSA. If Item 82 option "Casino/Card Club," "Insurance Company," or "MSB" is selected, the Item 78 entry must be "Internal Revenue Service (IRS)." If the financial institution filing the FinCEN SAR is subject to U.S. law and none of the other codes apply,

as may be the case[11] for non-bank residential mortgage lenders or originators, the entry must be "Internal Revenue Service (IRS)." If the FinCEN SAR is being filed by a government agency or if the financial institution filing the FinCEN SAR is not subject to U.S. law, the entry must be "Not Applicable".

- **"Financial institution identification" (Item 84)** – Select the option that identifies the financial institution entered in Item 79 (Filer name) and enter the identifying number in the text field. If "Research, Statistics, Supervision and Discount (RSSD)" is selected, but the identifying number is unknown, the information can be accessed at the Federal Financial Institutions Examination Council (FFIEC) Web Site at http://www.ffiec.gov/find/callreportsub.htm.
- **Address information for filing institution (Items 85-89)** – Enter the permanent street address for the financial institution entered in Item 79 (Filer name).
- **"Internal control/file number" (Item 91)** – To avoid an illegal disclosure of a FinCEN SAR, financial institutions often assign a unique internal control number/file number to each report, which law enforcement or regulatory agencies can reference without disclosing the existence or content of a particular FinCEN SAR. Use this field to reference any such assigned unique control number for the SAR.
- **"Law Enforcement (LE) contact information" (Items 92-95)** – If an LE agency was informed of the suspicious activity, enter the LE agency's contact information in Items 92-95.
- **"Filing institution contact office" (Item 96)** – Enter the name of the filing institution contact office where additional information about the FinCEN SAR or supporting documentation can be requested.
- **"Filing institution contact phone number" (Item 97)** – Enter the contact office telephone number and extension (if there is an extension).

Inquiries related to Items in Step 2 (Filing Institution Where Activity Occurred)

- **"Type of financial institution" (Item 47)** – *See Item 82 in Step 1 for answer to similar question.*

11. See FinCEN Administrative Ruling FIN-2012-R005 for clarification regarding the primary federal regulator of certain non-bank mortgage lenders and originators that are subsidiaries of federally regulated banks.

- **"Primary federal regulator" (Item 48)** – *See Item 78 in Step 1 for answer to similar question.*
- **"Financial institution identification" (Item 51)** – *See Item 84 in Step 1 for answer to similar question.*
- **"Financial institution's role in transaction" (Item 52)** – Check the box that describes the financial institution's role in the transactions identified in the suspicious activity as it pertains to the products or instruments checked in Items 39 and 40 (if both apply, check "Both"). For example, a money services business (MSB) selling money orders would choose "Selling location" while the same MSB would choose "Paying location" if it cashed the money orders involved in the suspicious activity. If the MSB both sold and cashed the money orders involved in the suspicious activity, it would select "Both". If neither choice is appropriate, please leave this Item blank.
- **Address information for where the activity occurred (Items 57-61)** – Enter the permanent street address for the financial institution entered in Item 53 (Legal name of financial institution). Leave Item 59 (State) blank if the state is unknown or the country is not the United States, Canada, or Mexico.
- **"Internal control/file number" (Item 62)** – *See Item 91 in Step 1 for answer to similar question.*
- **"Branch's role in transaction" (Item 64)** – *See Item 52 in Step 2 for answer to similar question.*
- **Address information for branch where activity occurred (Items 65-70)** – Enter the permanent street address for branch. If no branch was involved in the suspicious activity, check "If no branch activity involved, check this box" and leave Items 64-70 blank.

Inquiries related to Items in Step 3 (Subject Information)

- **Who is the subject? (Items 3-5)** – A subject is an individual or other entity potentially involved in the suspicious activity. Enter the individual's full name or the entity's legal name (for example, the legal name is the name on the articles of incorporation or other document that established the entity). Do not abbreviate names unless an abbreviation is part of the legal name.

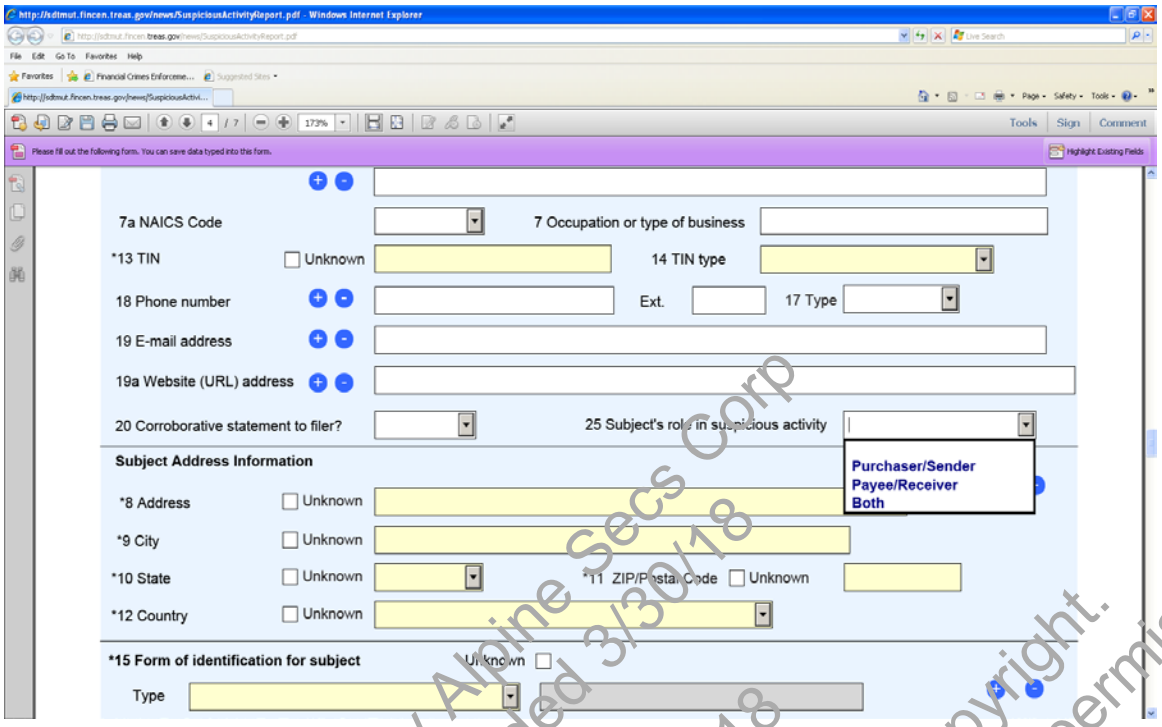
- **"NAICS Code" (Item 7a)** – Select the option that best identifies the occupation or type of business entered in Item 7 (Occupation or type of business). Filers can access the FinCEN-approved list of North American Industry Classification System (NAICS) codes from the BSA E-Filing Web Site at http://bsaefiling.fincen.treas.gov/main.html. If no selection from the NAICS code is appropriate, use a specific descriptive word or phrase, such as "Carpenter" or "Retired Carpenter" (but not simply "Retired") on the "Occupation" field and do not select a NAICS code.

- **"Relationship of the subject to an institution" (Item 21)** – If the subject has a relationship with a financial institution or individual listed in Step 1 or 2 of the FinCEN SAR, enter the financial institution's TIN in Item 21a (Institution EIN). Then select all options (21b through 21l) that describe the relationship. If the relationship is not covered by any of these options, select option 21z (Other) and enter a brief description of the relationship(s) in the "Other" text field.

- **"Status of the relationship" (Item 22)** – If Items 21h (Director), 21i (Employee), 21k (Officer), or 21l (Owner or Controlling Shareholder) is selected, indicate the status of relationship.

- **"Financial institution TIN and account number(s) affected that are related to subject" (Item 24)** – Enter information about any accounts involved in the suspicious activity that are related to the subject entered in Step 3 (Subject Information). An account is related to a subject if the subject owns the account, has control over the account, or conducted activity in or through an account the subject does not own or control. If no account has been identified as being related to the suspicious activity, check the "No known accounts involved" box. If the account is located at a foreign financial institution, check the "Non-U.S. Financial Institution" box. Enter all identifying numbers as a single text string without formatting or special characters such as hyphens or periods. If multiple financial institution TINs or accounts numbers are affected, the filer would click the "+" button to create additional Items.

- **"Subject's role in suspicious activity" (Item 25)** – Select the Item from the drop down menu that describes the subject's role in the suspicious activity as it pertains to the products or instruments checked in Items 39 and 40 (note: if both apply, check "Both").

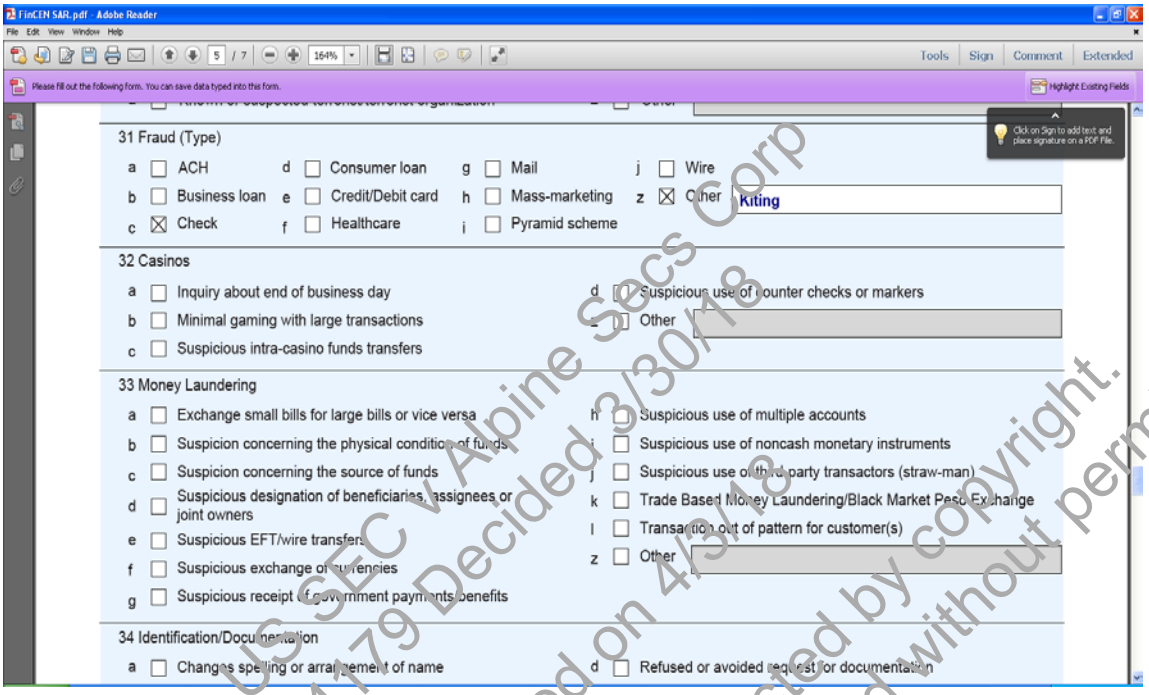


Inquiries related to Items in Step 4 (Suspicious Activity Information)

- **"Date or date range of suspicious activity for this report" (Item 27)** – Enter the suspicious activity date or date range for this report. If the suspicious activity occurred on a single day, enter that date in field 27a "From" and leave field 27b "To" blank. If the suspicious activity occurred on multiple days, enter the earliest date of suspicious activity in field 27a and the most recent date of suspicious activity in field 27b. If the exact date(s) of the suspicious activity is (are) unknown, enter a date range that the filer believes will encompass the date(s) of the suspicious activity.

- **What is the suspicious activity? (Items 29-40)** – Select all options that apply to the type of suspicious activity being reported. If a category applies but none of the options apply, check the "Other" box in that category and briefly describe the type of suspicious activity in the associated text field.

For example, if a financial institution needs to file a FinCEN SAR on kiting, they would check the "Other" box in Item 31 (Fraud) and type the word "Kiting" in the associated text field. For kiting associated with the use of checks, a financial institution also would select the "Check" box in Item 31 (Fraud).



Inquiries related to Step 5 (Narrative)

- **What is required when describing the suspicious activity identified?** The narrative is critical to understanding the suspicious activity being reported. How the narrative is written may determine whether the suspicious activity is clearly understood by investigators. Filers must complete the narrative in English and provide a clear, complete, and concise description of the suspicious activity. This narrative should include the data provided in the FinCEN SAR and any other information necessary to explain the suspicious activity. To assist, readers will find a separate article in the Issues & Guidance section of this issue that provides further guidance on constructing a SAR narrative.

Useful Links for completing the new FinCEN SAR

- Filing FinCEN's new Currency Transaction Report and Suspicious Activity Report (FIN-2012-G002) - http://www.fincen.gov/statutes_regs/guidance/html/FIN-2012-G002.html

- FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Requirements - http://bsaefiling.fincen.treas.gov/news/FinCENSARElectronicFilingRequirements.pdf

Suspicious Activity Report (SAR): Back to the Basics

By FinCEN's Office of Outreach Resources

SAR Basics

FinCEN is issuing a reminder to filing financial institutions of the importance of an accurate and complete Suspicious Activity Report. The SAR serves as a valuable investigative tool by providing information regarding previously unidentified accounts, potential illicit movement of monies and terrorist financing, and general lead information for financial crimes investigations. Filers and users of SARs are reminded that SARs are confidential. Similarly, information that would reveal the existence or non-existence of a SAR is confidential.

SAR Preparation

FinCEN, in consultation with other relevant federal regulatory authorities, has issued a guidance package[12] designed to assist financial institutions in the preparation of SARs and to improve the quality of information provided in SAR narratives.

SAR Narrative

The SAR Narrative remains a critical component of a SAR filing. However, with the flexibility of the suspicious activity section it was determined that fewer characters were necessary in the narrative section of the new SAR. Thus, the number of narrative characters has been limited to 17,000 characters (as compared to between approximately 39,000 and 49,000 characters in the legacy forms – depending on the SAR type). However, the narrative section allows filers to include an attachment that the financial institution believes would be useful to law enforcement.

12. http://www.fincen.gov/statutes_regs/guidance/html/FIN-2012-G002.html

Spreadsheet Attachments

The new SAR will accept a single, 1MB limited, comma separated value (CSV) attachment as part of the report. The CSV is a standard Microsoft file format that aids in reporting tabular data into a file format. This capability allows an institution to include data (such as specific financial transactions and funds transfers or other analytics), which is more readable and usable in this format than it would be if otherwise included in the narrative. Such an attachment will be considered a part of the narrative and is not considered to be a substitute for the narrative. As with other information that may be prepared in connection with the filing of a SAR, it can also be considered supporting documentation when not attached to the SAR and should be accorded confidentiality to the extent that it indicates the existence of a SAR.

Characterizations of Suspicious Activity

The new SAR is designed to accommodate the different types of industries that will file these reports. As such, the new SAR contains certain sections of suspicious activity characterizations which will generally be most relevant to a specific industry. When the filing institution's industry is selected in the discrete version of the report, other industries will be shaded out to signify a non-applicable status.[13]

In addition, the FinCEN's new SAR includes a number of additional data elements pertaining to the type of suspicious activity and the financial services involved. The decision to include these additional data elements in the FinCEN SAR arose from extensive discussions with law enforcement officials. It was determined that the inclusion of such elements would facilitate more effective use of the information collected in the reports. FinCEN acknowledges that the expansion of these characterizations may create the need for clarification on how to select among the choices provided to depict the activity, as well as how to describe this information in Part V, the narrative.

13. As an example, if the filer is a broker-dealer, then insurance and casino selections may be grayed out; if the filer is a depository institution, then casino and the broker-dealer selections are grayed out. The full implementation of this capability is still being developed. Filers may choose to enable and use these fields, as necessary, for example, in reporting activity that involves affiliated institutions across industry sectors. Institutions that batch file their reports may not have this feature, based on software design.

Critical Fields

Certain fields in the new SAR are marked as "critical" for technical filing purposes; for discrete filers, the BSA E-Filing System will not accept filings in which these fields are left blank.[14] For these items, the filing institution must either provide the requested information or affirmatively check the "unknown" (Unk.) box if that box is provided for in a critical field. This unknown box will supersede FinCEN's previous guidance requesting that filers input "NOT APPLICABLE," "UNKNOWN," "NONE," or "XX" in certain fields. For those fields that are not marked as "critical" for technical filing purposes, the BSA E-Filing System will accept reports in which these fields have been left blank. FinCEN expects that financial institutions will provide the most complete filing information available within each report consistent with existing regulatory expectations regardless of whether or not the individual fields are deemed critical for technical filing purposes (i.e., filers must either select the "unknown" box or input the correct information on the report even if the field is not considered a critical field.)

Gender Field

FinCEN has been asked for guidance on the "Gender" Field (Item 4 of Part I: Subject Information). Based on feedback from law enforcement officials, information related to the gender of the subject could be an important characteristic for query purposes. However, FinCEN has not designated the "Gender" field as mandatory.

NAICS Code

FinCEN has also been asked for guidance on the use of the North American Industry Classification System (NAICS) code field (Item 7a). Law enforcement officials have indicated that the NAICS code is beneficial in SAR data. Note: financial institutions are not required to become familiar with NAICS codes, as the appropriate list of codes is contained in a drop down menu that automatically populates the field. In addition, use of a NAICS code is not mandatory, and a financial institution may still provide a text response with respect to this information.

14. Batch filers will be notified via the acknowledgement process that critical field errors were made and should be corrected.

Fields Related to Internet Presence

The FinCEN SAR includes certain new elements related to the internet presence of subjects and suspicious activity, specifically the "E-mail address" and "Website (URL) address" fields within Part I: Subject Information and "IP address (if available)," in Part II: Suspicious Activity Information. These are items which many filers have previously included in the narratives of the legacy SARs in the context of describing suspicious activity. For example, to show that suspected criminal activity was being conducted from a specific internet site location. By providing a discrete space into which such information may additionally be entered, the new reports will facilitate FinCEN's and law enforcement's ability to make connections between elements reported across separate filings and external data sources. In doing so, FinCEN does not intend to create any obligation or expectation that financial institutions would collect this information as a matter of course. The narrative section of the report may be used to provide more information as to how an internet presence relates to the suspicious activity or to provide any other relevant email or IP addresses that may pertain to non-subjects.[15]

Writing Effective SAR Narratives

By FinCEN's Office of Outreach Resources

When preparing a Suspicious Activity Report (SAR), filers complete fields on the SAR that contain information about the subject(s) of the filing, such as their name and address, and the activity being reported, such as the characterization of the suspicious activity. They also report other information such as when the activity occurred, the dollar amount involved, and other information that help users of the data identify the filer, and identify, investigate or analyze the activity being reported. The narrative is a critical part of the SAR because it is the where the filer can summarize and provide a more detailed description of the activity being reported. For that reason, it is essential that the narrative be clear, complete and thorough.

In this article we include examples of SARs reporting more routine activity that a filer might identify – potentially unregistered MSB customers and counterfeit checks. We explain why a particular example is more or less effective as a SAR narrative.

15. http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2012-G002.pdf

The Importance of the SAR Narrative

As noted in the article *Suspicious Activity Report: Back to the Basics*, the size of the narrative field has been reduced in the FinCEN SAR. Other sections of the FinCEN SAR have been expanded to allow for filers to provide additional information in those parts of the report, such as additional check boxes to characterize the suspicious activity being reported. Even though, as noted, the narrative remains a critical part of the FinCEN SAR, filers should consider the reduced size of the narrative section, and the expanded fields in other parts of the form, and utilize the narrative in such a manner as to maximize the value of the information being provided in that section.

When writing a narrative, filers should aim to expand upon the information provided in the other parts of the FinCEN SAR and provide any additional information needed to address five essential elements of information – *who? what? when? where?* and *why?* – about the suspicious activity being reported:

Who is conducting the suspicious activity?

Part I of the SAR instructs the filer to provide specific information about the subject(s) of the filing. In the SAR narrative, the filer can further describe the suspect(s), such as occupational information, including position or title, and the nature of the suspect's business. The SAR narrative should also include any known relationships among subjects reported on the SAR or businesses identified in the narrative. While detailed subject information may not always be available (i.e., situations involving non-account holders), filers should include as much information as is known to them about the subject(s).

What instruments, methods or mechanisms are being used to facilitate the suspect transaction(s)?

An effective SAR narrative describes how the subject(s) conducted the illicit activity, including what instruments, methods or mechanisms were used. For example, whether shell companies were suspected as being either the sender or beneficiary of a wire transfer, or whether the subject(s) used the Internet or Remote Deposit Capture to initiate the activity.

When did the suspicious activity take place?

If the activity takes place over a period of time, indicate when the suspicious activity first occurred and the history of the suspected illicit activity. To better understand the history and nature of the activity, and the flow of funds, filers should provide information on each individual transaction (i.e., dates and amounts.) The ability to include attachments in the new FinCEN SAR can help filers in providing this data is a more user friendly format than allowed for in the legacy SAR.

Where did the suspicious activity take place?

Filers should indicate any offices or branches of their financial institution that the suspicious activity occurred at or through, and provide the addresses of those locations. Filers should also specify whether the activity involved a foreign jurisdiction, such as funds wired overseas, and the foreign jurisdiction and/or financial institution involved, as well as any account numbers associated with the subject of the suspect transaction(s).

Why does the filer think the activity is suspicious?

In answering this question, a filer should describe why the transaction is unusual for the customer or why the activity created a red flag for the filer or triggered an alert within their system. These answers will vary based on the filer's institution type (for example, a depository institution vs. an insurance company) and so a filer should also consider the types of products and services they offer, what they know about the type of accounts the customer has with the institution and the normally expected business activity of the customer (if they are a customer of the filer), and why this is not normal or expected activity.

Reporting Potentially Unregistered MSBs

More effective SAR narrative:

A review of activity in an account for Stop In, Inc. indicates a possible unregistered or unlicensed money services business. This review was conducted based on a report indicating unusual or potentially suspicious activity based on the customer profile. Stop In, Inc. has been a bank customer since 5/21/2011. Business checking account number 580214566 was reviewed for this case. The account was opened at the Lake Road branch on 5/21/2011. Samuel Jones is an authorized signer on this account. Transaction activity from 5/21/2011 to 8/13/2011 was reviewed and revealed 49 deposits totaling $87,856.40. The deposits included 23 third party checks. Deposits also included nine personal checks for more than $1,000. Two third party checks have been returned for $1,785 and $2,205. Cash made up 15% of all dollars deposited and almost 68% of all dollars withdrawn from the account during the period of this review. No wire transfers were detected. Account activity does not show the expected business expenditures for utilities and rent. Research via the internet and through commercial database sources revealed no additional pertinent information about the customer. Bank records revealed Stop In, Inc. doing business as a convenience store, Stop-In Food Mart, at Rt. 1 and Lake Road. Per bank records, Stop In, Inc.'s taxpayer identification number is 01-2345677. Bank records also revealed that neither Stop In, Inc. nor Stop-In Food Mart is registered with FinCEN as a money services business. They are licensed by the state of Virginia to cash checks. The business account was closed for failing to indicate it was operating as an MSB, a violation of bank account opening policy. Supporting documentation is available upon request. For assistance, contact the AML/Fraud Unit at 888-999-7777, or amlfraud@xbank.com. Please reference AML Case 2011-XXX.

Why this SAR narrative is more effective:

This SAR narrative explains why the filer believed the customer was an unregistered check casher by the type of activity occurring in the account (deposits of third party checks and checks over $1,000, and large cash withdrawals). The filer describes when the activity occurred and the transaction amounts involved. The filer also provides details about the customer, including its legal name and the name under which it conducts business, the businesses address, type of business, the date the

account was opened, the account number and its licensing and registration status at the time of this filing. The filer also identifies at which branch the customer banked, who should be contacted at the bank for supporting documentation, and how to reference the case.

Less effective SAR narrative:

> First Federal Bank is filing this SAR in connection with possible suspicious payments to ABC Corporation originating from XYZ LLC. This review of the transactions that led to the filing of this SAR was prompted by an alert from the bank's payment monitoring system for Century Bank concerning transfers on behalf of its client XYZ LLC. Century Bank is a correspondent-banking client of First Federal. First Federal records reveal that from June 29, 2011 to August 1, 2011, 4 payments totaling $13,675.21 were transmitted to ABC Corporation at Century Bank. ABC Corporation is being used to repatriate funds to Venezuela. As of March 2, 2012, ABC Corporation does not appear on FinCEN's MSB registration list.

Why this SAR narrative is less effective:

This SAR reported the subject as a potential dealer in foreign exchange, and indicates that the subject is being used to repatriate funds to Venezuela, but it does not describe how this is occurring or what led the filer to suspect it was occurring. What in the filer's monitoring system drew their attention to the payments sent to the subject by XYC LLC – were they not expected business transactions, or not from an expected source of funds? What did ABC Corporation do with the funds once they were received? What was it about these payments that led to the filer to suspect it was being used to repatriate funds to Venezuela? More detail will help users of the data better understand the nature of the suspected illicit activity and how it is occurring, and can help identify additional potential suspects or links to other illicit activity.

Reporting Counterfeit Check Activity

More effective SAR narrative:

On June 22, 2010, East Valley Bank, a subsidiary of Mountain Bank, referred this counterfeit check activity to the Mountain Bank Compliance Department involving an account held in the name of Daniel Alan Parker, account number 20808156. Account number 20808156 was opened on May 14, 2010 with an initial deposit of $500. On June 5, 2010, Mr. Parker deposited a check in the amount of $295,650.20, payable to Daniel Parker, Dallas, TX, from Texas Title, Inc. Escrow Account as maker, drawn on Central Bank ("Central"), routing and transit number 99990008, account number 6786812882. Mr. Parker requested and received $8,500 in cash from the deposit. On June 14, 2010 a bank employee responsible for reviewing large transactions suggested that the teller request the return of the $8,500 cash given to Mr. Parker until the check was paid by Central. Mr. Parker stated that he would be "more than happy" to return the funds but could not return to the bank until possibly June 17. In the meantime, the teller contacted Central Bank to verify the check and was told that the funds were available at that time. On June 22, Central Bank notified East Valley Bank that the check was fraudulent. The teller again contacted Mr. Parker and requested the return of funds provided to him from the deposit. Mr. Parker stated that he had become uncomfortable about the validity of the check after speaking to the teller and that he had contacted Central Bank. He believed his call to Central prompted them to notify East Valley of the fraudulent item. The teller again asked Mr. Parker to return the funds. Contrary to his earlier agreement, Mr. Parker informed the teller that he could not return the funds as he had already used the funds to pay medical bills. Mr. Parker assured the teller that he was expecting a wire transfer that would be in excess of the amount of the counterfeit check. As of July 29, 2010, no such wire transfer has been received and the account remains overdrawn. It appears as through Texas Title, Inc or an individual purporting to represent such company, counterfeited such check in an attempt to defraud Mr. Parker and/or East Valley Bank. It also appears as though Mr. Parker made false statements to bank employees regarding the existence of an anticipated wire transfer in an attempt to defraud the bank. East Valley anticipates a loss in the amount of $7,300, the negative balance of Mr. Parker's account. SAR supporting documentation retained includes internal correspondence, copy of the counterfeit check and account statements.

Why this SAR narrative is more effective:

This narrative describes how the subject opened the account on May 14 with a small deposit followed very shortly by a large deposit that led to the subsequent suspicious activity. The filer explains the source of the funds and how they came to learn that the check was fraudulent. They also explain in detail their exchanges with the subject and the subject's actions that led them to believe that he might be a party to the suspicious activity.

Less effective SAR narrative:

> The purpose of this SAR is to report a counterfeit check payable to Mark Evans for $14,620 was deposited into the sole account of Mary Louise Evans, Charter State Bank account number 65697142, on 4/5/11. The check was drawn on the National Bank account of Dynamic Tech, Inc. The maker of the check is Elizabeth Thomas. Mark Evans endorsed the check over to Mary Louise Evans. A hold was placed on the funds. On 4/13/11 the check was returned unpaid as unable to locate. National Bank confirmed the check is counterfeit. Mark Evans stated he received the check via FedEx from Alex Jones as payment for a vehicle he had listed for sale on Craigslist. No loss was sustained due to the hold.

Why this SAR narrative is less effective:

This SAR listed only the account holder, Mary Louise Evans, as the subject; however, the narrative does not describe the account holder's role in the activity being reported – other than being the recipient of the endorsed check. As described in this narrative, Mark Evans, Elizabeth Thomas and/or Alex Jones would seem to be subjects in this reported activity and the bank should have considered listing them as subjects as well, with as much information as is known on those subjects. This narrative also does not explain the connection between the check being drawn on Dynamic Tech and the sale of a vehicle through an Internet site and why this is relevant.

Use of key terms

Using clear, concise terms assists users of FinCEN data in identifying the suspicious activity being described in the SAR narrative. Certain FinCEN Advisories have recommended the use of key terms to identify particular activities, such as use of the term "tax refund fraud" described in FinCEN Advisory–FIN-2012-A005,

Tax Refund Fraud and Related Identity Theft. The use of short, concise phrases, such as "unregistered MSB" or "unlicensed check casher," is also helpful in more quickly identifying activity being reported. Additional information on key terms is available at http://www.fincen.gov/news_room/advisory/AdvisoryKeyTerms.html.

Use of attachments

Filers using the legacy SAR forms cannot include attachments when filing a SAR. The new FinCEN SAR will allow filers to include a single, comma separated value (CSV) attachment with their SAR filing. This attachment would be part of the narrative, but not a substitute for the narrative. The attachment functionality will allow filers to include data, such as a list of counterfeit checks, in a more readable and usable format. The file can also be considered supporting documentation when not attached to the SAR.

For additional information on the new SAR, see the articles "SAR Activity Review: Back to the Basics" and "Analysis of Suspicious Activity Report (SAR) Inquiries Received by FinCEN's Regulatory Helpline" included in this issue. Additional information on the new SAR and the new CTR can also be found on FinCEN's website at http://www.fincen.gov/whatsnew/html/20120329.html.

Industry Forum

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into an aspect of compliance management or fraud prevention. In this issue, we get an industry perspective on the AML risks presented by Business Funded Prepaid Cards. The *Industry Forum* section provides an opportunity for the industry to share its views. The information provided may not represent the official position of the U.S. Government.

Taking a Second Look at AML Risks from Business Funded Prepaid Cards: It's a Whole New Ball Game

By Judith Rinearson, Bryan Cave LLP
Regulatory Counsel, Network Branded Prepaid Card Association (NBPCA)[16]

Introduction

Prepaid cards are generally considered a higher risk payment product (as compared to credit and debit cards) and the recent Prepaid Access regulations issued by FinCEN do a solid job at addressing those risks. But an important subset of prepaid card products were not discussed and perhaps not even contemplated when the Prepaid Access regulations were developed: prepaid cards purchased, issued or loaded solely by businesses ("Business Funded Cards"). These cards represent a very different set of risk and compliance issues – and deserve a fresh look. (Yes, it's a "whole new ball game.") This article discusses the range of business funded prepaid card products, the risks arising from such products, how such products are currently addressed under the Prepaid Access regulations, and suggests some best practices for issuing banks, providers and sellers of such products.

16. Judith wishes to thank Kristine M. Andreassen of Bryan Cave's Washington, D.C. office for her assistance in preparing this article. Although Judith serves as Chair of the NBPCA Government Relations Working Group and as the NBPCA representative on BSAAG, the views and opinions set forth in this article are her own and should not be attributed to the NBPCA or its members.

What are Business Funded Cards?

The term "Business Funded Cards" encompasses a broad range of prepaid card programs that are funded *solely* by corporations, financial institutions, employers, and other business entities of all kinds to make payments. These payments were traditionally made in the form of checks (or paper gift certificates), which is expensive for the business and, in many cases, inconvenient for the recipient.

Business Funded Cards can include both "closed loop" cards issued by retailers[17] (for example, when a business purchases 100 gift cards from a local restaurant to give to employees or customers during the holidays) as well as "open loop" cards issued by banks and financial institutions[18] (for example, when employees are issued payroll cards to receive their wages).

Below are examples of some of the different types of Business Funded Card programs that exist today. Please note that not all of these Business Funded Card programs are "reloadable." Certain incentive payments, gifting programs, wellness payments, bonuses, insurance claim payments and disaster relief payments are often one-time payments that do not involve reloading by either the business or the recipient.

1. Business Funded Cards in which the funds are "owned" by the recipient to whom the card is issued. Certain prepaid cards replace checks that are paid from a business to an individual, for funds that are owed by the business to, and belong to, the recipient. Examples where funds on a prepaid card are ultimately owed to, and owned by, an individual include:

   a. Benefits, incentives, wages, salaries, commissions or bonuses paid to employees, vendors, distribution channel partners, or independent contractors.

   b. FSA, HSA and HRA arrangements, and employee wellness programs.

   c. Per diem allowances for employees' travel expenses (where any amount under the daily allowance is kept by the employee).

17. The term "closed loop" card generally refers to prepaid cards that are issued for limited purposes and can only be used at a single retailer or retail chain, or at a single website to make purchases, and cannot be used to access cash. Retailer-issued gift cards, such as Home Depot cards or Starbucks cards, are typical closed loop prepaid cards.

18. The term "open loop" card generally refers to prepaid cards that are issued by a bank or financial institution, display a payment network brand on the front (Visa, MasterCard, American Express or Discover) and can be used widely to make purchases where that brand is accepted and/or to obtain cash at ATMs.

d. Reimbursements to employees, vendors or contractors who have incurred business expenses.

e. Disbursement of insurance claims paid to individuals.

f. Disaster relief payments to individuals.

2. Business Funded Cards in which the funds are still "owned" by the business and do not belong to the recipient to whom the card is issued. Examples where funds on prepaid cards generally belong to the business include:

   a. Cards given to a company's employees to use for future business expenses. This may be an alternative to issuing company credit cards to employees, or having employees pay expenses themselves and submit for reimbursement. Examples include purchasing cards or travel expense cards.

   b. Cards given to a company's independent contractors to use for future business expenses. Example: Purchasing Cards used to obtain building materials by a general contractor making repairs at the company's office.

   c. Cards given to a company's vendors (businesses) for accounts payable payments or reimbursements. For example, trucking companies often provide cards to drivers for fuel and repairs. The card may be embossed with the company's name instead of the driver's name and the company funding the card may not know which individual(s) will ultimately use the card.

3. Business Funded Cards in which the funds are granted by the business to a customer temporarily as an incentive, reward or promotional item, but are not "owned" by the customer and may revert back to the business if they are not used under the terms of the promotional, reward or incentive program. Examples where funds do not represent an obligation owed to an individual, but the ability to use the card often for a limited period (versus ownership of funds) include:

   a. Marketing reward or loyalty programs. These include gift cards issued by retailers based on previous shopping or accrued loyalty points.

   b. Promotions, giveaways and rebates. These include "gift with purchases" or gift cards used to promote the purchase of a manufacturer's product or a specific travel destination.

It is important to note that this discussion of Business Funded Cards addresses only cards that are funded solely by the business. Some prepaid cards combine two attributes – they are both business funded and consumer funded. For example, there are payroll cards that are "portable." In addition to receiving the employee's payroll or wages from the employer, the employee has the option of loading his or her own funds onto the payroll card, and can keep and continue to use the payroll card even when moving to a new employer. Such cards pose different risks and are not intended to be included within the scope of this article.

What Risks Arise from Business Funded Cards?

There are many factors that go into a risk assessment of Business Funded Cards. However, taken as a whole, this group of prepaid payment products tends to pose less risks than consumer funded cards for one critical reason: the source of funds is known. This is particularly true for open loop cards which are issued by banks or similar financial institutions and which are acquired or purchased by publicly traded corporations.[19]

One factor that makes Business Funded Cards so different from consumer funded cards is that, with Business Funded Cards, it is actually more important to know your business customer than it is to know the ultimate cardholder. It is the business, not the cardholder, that is the source of funds, and any misuse of Business Funded Cards primarily derives from false business fronts, shell corporations, and other criminal efforts to disguise the business ownership, purpose and/or source of funds. For these customers, the biggest risk arises from the failure to adequately identify and verify, and collect other information about, the business itself.

Banks that are familiar with Business Funded Card programs understand the importance of knowing their business customers that purchase prepaid cards. Under standard bank procedures, a business that wishes to obtain and load prepaid cards for its employees, customers or business partners becomes the direct customer of that bank. The business (including its source of funds) is vetted by the bank both initially and on an ongoing basis. Both Customer Identification Program (CIP) and Customer Due Diligence (CDD) procedures are performed on the business, often including the review of publicly available information, financial statements, references, and information about the business' owners and/or management, as well as understanding the purpose for the business' acquisition of open loop prepaid cards and the expected usage of such cards.

19. Although open loop prepaid cards can be issued by a range of regulated financial institutions, including banks, savings associations, credit unions, and some licensed money transmitters, for purposes of this article, we will refer to these all as "banks."

Closely tied to the CIP/CDD process, banks that issue and distribute Business Funded Cards also perform back-end monitoring of transactions. This is a critical part of a bank's AML program. For example, Business Funded Cards that are distributed to cruise line passengers as part of their travel package would be expected to be used in the Caribbean; Business Funded Cards issued for expense reimbursement purposes to construction workers in Des Moines would not.

Other factors that determine the level of risk posed by a Business Funded Card program are (i) whether the cards can be used to access cash; and (ii) whether the cards are reloadable. In many cases, especially in reward and promotional programs, Business Funded Cards are not reloadable nor can they be used to access cash. Such cards do not have many of the functionalities of general purpose reloadable (GPR) prepaid cards and certainly do not function like bank account substitutes.

Can Business Funded Cards be misused? Of course they can. As noted above, there are some examples of the misuse of Business Funded Cards – but these cases generally involve the failure to perform solid CIP and due diligence on the business involved – not the individual cardholder. Some examples of misuse of Business Funded Cards include:

- A Black Market Peso Exchange operation involving a crooked program manager who set up payroll card programs for fake companies.[20] $39 million was withdrawn from these fake payroll cards at a single ATM in Colombia from 2006 to mid-2007.
- A company layered funds for clients (criminal enterprises) and transferred those funds overseas. All clients had prepaid cards onto which funds could be delivered (some had 1 card, others had 50 or 100 cards). Cards from three different crooked program managers were involved.
- A Black Market Peso Exchange operation involving a "multi-level marketing scheme" through which customers could purchase prepaid cards to buy electronics and other items at affiliated retail stores.[21]

20. Some of these examples also demonstrate the importance of banks performing thorough due diligence on its third party service providers. This crucial issue has been well documented. *See, for example*, OCC Bulletin 2001-47; FFIEC Interagency Statement on Risk Management of Outsourced Technology Services; OTS Thrift Bulletin 82a; FDIC FIL-44-2008; and BSA Exam manual.

21. See http://www.justice.gov/dea/pubs/states/newsrel/2009/nyc102309.html.

- A cleaning company allegedly put job applicants on its payroll without their knowledge. Payroll cards and PINs for these "ghost" employees were sent directly to the cleaning company.[22]

These above examples demonstrate the importance of performing careful and effective customer identification and due diligence for business customers loading or purchasing Business Funded Cards.

What Do the Prepaid Access Regulations Require for Business Funded Cards?

The Prepaid Access regulations require providers and sellers of prepaid access, as part of their AML programs, to "establish procedures to verify the identity of a person who obtains prepaid access under a prepaid program and obtain identifying information concerning such a person, including name, date of birth, address, and identification number."[23] The use of the term "obtains" is a little unclear, because it could apply to the purchaser as well as to the ultimate end-user of a Business Funded Card. Perhaps this is an area where further clarification can be provided, because in many instances the end-user is not the customer of the issuing bank, nor is he or she a "customer" of the provider or seller of the prepaid access in any traditional sense.

In the preamble to the Prepaid Access regulations, FinCEN states the following regarding the identification and verification requirements:

> This regulation adds a customer information recordkeeping requirement (including name, address, date of birth, and identification number) for the provider and seller of prepaid access.
>
> * * * * *
>
> FinCEN believes that obtaining and retaining (or retaining access to) such customer information is necessary for greater financial transparency concerning the purchasers of prepaid access.
>
> * * * * *

22. See http://www.ice.gov/doclib/aml/pdf/2009/murray.pdf at 12-14.
23. 31 CFR 1022.210(d)(1)(iv), emphasis added.

> These requirements are intended to mirror the customer identification programs required of other financial institutions and draws on the explanations and interpretations issued with respect to those requirements.
>
> * * * * *
>
> Providers and sellers of prepaid access are reminded that the AML programs they develop pursuant to this rule should be appropriate for their prepaid operations.[24]

For Business Funded Cards, it is the business, not an individual, that is the source of funds and that purchases the prepaid access. That is why the question must be asked: "Who is the person that has 'obtained' the prepaid access when the product is a Business Funded Card?" Using a risk-based approach, collecting and verifying the cardholder's personal information on a blanket basis many not be appropriate for all cardholders with Business Funded Cards – especially when the business-funded cards cannot be reloaded or do not access cash. In this regard, it should be noted that in a traditional bank account opened for a business, the bank's CIP obligation clearly relates to the business and not to the business' individual customers or employees who may receive checks from that business.[25] Moreover, in most instances, the risk of abuse of Business Funded Cards for money laundering and terrorist financing purposes lies predominantly with the business that is funding the cards, not the individual who may ultimately spend those funds. If a provider's AML program is to be "appropriate" for its operations, then it is certainly crucial that identification/verification should be performed on the business obtaining the prepaid access.

What Are Some Recommendations for Banks, Provides and Sellers involved with Business Funded Card programs?

Business Funded Cards do pose some risks and best practices dictate that certain procedures should be followed by banks, providers and sellers that wish to issue, promote and distribute Business Funded Card products. Here are some suggestions:

- Thorough due diligence must be performed on the business that is the source of funds. Depending on the business and the product(s) involved, this might involve checking Secretary of State incorporation/formation records, reviewing

24. 76 Fed. Reg. 45404, 45413 (July 29, 2011), emphasis added.

25. See 31 CFR 1010.220.

public filings with the Securities and Exchange Commission or other sources, obtaining references or running credit and/or background checks. The larger the purchase, the more closely the business should be scrutinized.

- For Business Funded Cards issued through an employer, collection of the individual cardholder's (i.e., employee's) identifying information and identity verification is done by the employer, via the I-9 process. Issuing banks or providers that rely on the employer's I-9 processes should perform due diligence not simply on the identification and verification of the employer, but also on the employer's internal procedures in order to ensure that the employer follows a effective I-9 process, retains the records, and can provide access to the bank or provider upon request. Adherence to these procedures must also be audited from time to time. For example, some issuers or providers do annual "spot checks" by requesting the employers provide I-9 files for a small sampling of payroll cardholders to ensure that such files are complete and available. By not requiring all data to be transferred to the issuing bank and/or provider, the risk of data security and privacy breaches may also be reduced.
- For sales incentives and similar programs, collection of identifying information and identity verification is done on the sales reps by the company that employs the sales reps. The program sponsor (e.g., a manufacturer) would have performed its own due diligence on the company that employs the sales reps and the card issuer would have access to the program sponsor's data on an as needed basis. Again, as a best practice, issuing banks and providers should include in its due diligence process a review of the kinds of data the program sponsor itself collects and verifies, and ensure that the bank/provider has access to the data if needed.
- For certain Business Funded Card programs where cards are delivered to specific customers as part of loyalty or promotional programs, some identifying information is generally collected from the customer via a participation or enrollment form. For example, when a telecommunications company offers a rebate to customers for purchasing a particular mobile phone, the customer will have to meet certain eligibility criteria and have an account with the telecom company. During that account opening process, identifying information is collected about the customer, and some form of verification may be performed as well. These cards also pose significantly lower risks because they are generally lower value disposable cards that cannot be reloaded, cannot access cash and cannot be used internationally.

- For all prepaid card programs, including Business Funded Cards, transactional activity should be monitored on a regular basis for unusual activity such as high dollar loads, high dollar spend, MCC code restrictions and international activity, as well as any activity that conflicts with the stated purpose of the card program.
- For bulk purchases of "closed loop" cards, especially in amounts exceeding $10,000, the issuing retailers should also collect information about the business that is purchasing the cards, the purpose of the purchase, and expected usage, and should monitor use to make sure it does not conflict with the stated purpose of the card program.

Conclusion

Business Funded Cards can be "win-win-win" products that benefit prepaid card issuers, providers and sellers, as well as the businesses that fund them, and the recipients who use them. Both bank and MSBs that offer such cards should establish appropriate risk-based AML compliance programs that take into account the very unique and different risks posed by such products.

Feedback Form

Financial Crimes Enforcement Network

U.S. Department of the Treasury

Tell Us What You Think

Your feedback is important and will assist us in planning future issues of *The SAR Activity Review*. Please take the time to complete this form. The form can be faxed to FinCEN at (202) 354-6411 or accessed and completed online at http://www.fincen.gov/feedback/fb.sar.artti.php.

Questions regarding *The SAR Activity Review* can be submitted to sar.review@fincen.gov. For all other questions, please contact our Regulatory Helpline at (800) 949-2732. **Please do not submit questions regarding suspicious activity reports to the SAR Activity Review mailbox.**

A. Please identify your type of financial institution.

Depository Institution:
__ Bank or Bank Holding Company
__ Savings Association
__ Credit Union
__ Foreign Bank with U.S. Branches or Agencies

Money Services Business:
__ Money Transmitter
__ Money Order Company or Agent
__ Traveler's Check Company or Agent
__ Currency Dealer or Exchanger
__ Prepaid Access

__ **Insurance Company**
__ **Dealers in Precious Metals, Precious Stones, or Jewels**
__ **Other** (please identify): _____

Securities and Futures Industry:
__ Securities Broker/Dealer
__Futures Commission Merchant
__Introducing Broker in Commodities
__Mutual Fund

Casino or Card Club:
__ Casino located in Nevada
__ Casino located outside of Nevada
__ Card Club

B. Please indicate your level of satisfaction with each section of this issue of *The SAR Activity Review- Trends Tips and Issues* (circle your response).

	1=Not Useful, 5=Very Useful				
Section 1 - Director's Forum	1	2	3	4	5
Section 2 - Trends and Analysis	1	2	3	4	5
Section 3 - Law Enforcement Cases	1	2	3	4	5
Section 4 - Issues & Guidance	1	2	3	4	5
Section 5 - Industry Forum	1	2	3	4	5

C. What information or article in this edition did you find the most helpful or interesting? Please explain why (please indicate by topic title):

_____
_____
_____
_____

D. What information did you find least helpful or interesting? Please explain why (again, please indicate by topic title):

_____
_____
_____
_____

E. What new TOPICS, TRENDS, or PATTERNS in suspicious activity would you like to see addressed in the next edition of *The SAR Activity Review - Trends, Tips & Issues*? Please be specific, for example: information on a certain type of activity, or an emerging technology of interest.

_____
_____
_____
_____

F. What other feedback does your financial institution have about The SAR Activity Review publication itself?

_____
_____
_____
_____

G. How often do you read the SAR Activity Review? (Check all that apply)

[ ] Every Issue
[ ] Occasionally
[ ] Only issues with content directly applicable to my industry or area of interest